McAfee Host Intrusion Prevention 8.0

Installationshandbuch

COPYRIGHT

Copyright © 2010 McAfee, Inc. Alle Rechte vorbehalten.

Diese Publikation darf in keiner Form und in keiner Weise ohne die schriftliche Genehmigung von McAfee, Inc., oder ihren Lieferanten und angeschlossenen Unternehmen ganz oder teilweise reproduziert, übermittelt, übertragen, in einem Abrufsystem gespeichert oder in eine andere Sprache übersetzt werden.

MARKEN

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD sind eingetragene Marken oder Marken von McAfee, Inc. und/oder der Tochterunternehmen in den USA und/oder anderen Ländern. Die Farbe Rot in Verbindung mit Sicherheit ist ein Merkmal der McAfee-Produkte. Alle anderen eingetragenen und nicht eingetragenen Marken in diesem Dokument sind alleiniges Eigentum der jeweiligen Besitzer.

INFORMATIONEN ZUR LIZENZ

Lizenzvereinbarung

HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN LIZENZVERTRAG FÜR DIE VON IHNEN ERWORBENE SOFTWARE SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN SOFTWARE-LIZENZTYP SIE ERWORBEN HABEN, SCHLAGEN SIE IN DEN UNTERLAGEN ZUM KAUF UND WEITEREN UNTERLAGEN BEZÜGLICH DER LIZENZGEWÄHRUNG ODER DEN BESTELLUNTERLAGEN NACH, DIE SIE ZUSAMMEN MIT DEM SOFTWAREPAKET ODER SEPARAT (ALS BROSCHÜRE, DATEI AUF DER PRODUKT-CD ODER ALS DATEI, DIE AUF DER WEBSEITE VERFÜGBAR IST, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN) ERHALTEN HABEN. WENN SIE MIT DEN IN DIESER VEREINBARUNG AUFGEFÜHRTEN BESTIMMUNGEN NICHT EINVERSTANDEN SIND, UNTERLASSEN SIE DIE INSTALLATION DER SOFTWARE. SOFERN MÖGLICH, GEBEN SIE DAS PRODUKT AN MCAFEE ODER IHREN HÄNDLER BEI VOLLER RÜCKERSTATTUNG DES KAUFPREISES ZURÜCK.

Inhaltsverzeichnis

Installieren von McAfee Host Intrusion Prevention **5**

Komponenten 7

Installationsübersicht 7

Neuheiten in dieser Version 9

Bewährte Vorgehensweisen für einen einfachen Weg zum Erfolg **11**

1. Entwickeln einer Strategie 13

2. Vorbereiten einer Pilotumgebung 17

3. Installieren und Konfigurieren 19

4. Grundanpassung 21

5. Aktivieren des adaptiven Modus (optional) 25

6. Feinabstimmung 26

7. Ausführen der Wartung und Erweiterung 27

Installieren von ePolicy Orchestrator **29**

Installieren der Erweiterung 30

Entfernen der Erweiterung 31

Migrieren von Richtlinien **32**

Migrieren von Richtlinien aus früheren Versionen 33

Migrieren von Richtlinien über eine XML-Datei 34

Installieren des Windows-Clients **35**

Details zum Windows-Client 35

Remote-Installation des Windows-Clients 37

Lokale Installation des Windows-Clients 38

Anwenden von Richtlinien und IPS-Inhaltsaktualisierungen 38

Entfernen des Windows-Clients 39

Fehlerbehebung bei Windows-Installationsproblemen 39

Anhalten des Windows-Clients 41

Neustarten des Windows-Clients 41

Installieren des Solaris-Clients **42**

Details zum Solaris-Client 42

Remote-Installation des Solaris-Clients 44

Lokale Installation des Solaris-Clients. 44
Anwenden von Richtlinien und IPS-Inhaltsaktualisierungen. 45
Entfernen des Solaris-Clients. 45
Fehlerbehebung bei Solaris-Installationsproblemen. 45
Anhalten des Solaris-Clients. 46
Neustarten des Solaris-Clients. 46

Installieren des Linux-Clients. 48

Details zum Linux-Client. 48
Remote-Installation des Linux-Clients. 50
Lokale Installation des Linux-Clients. 51
Anwenden von Richtlinien und IPS-Inhaltsaktualisierungen. 52
Entfernen des Linux-Clients. 52
Fehlerbehebung bei Linux-Installationsproblemen. 53
Anhalten des Linux-Clients. 53
Neustarten des Linux-Clients. 54

Installieren von McAfee Host Intrusion Prevention

Mit diesem Handbuch werden alle Informationen bereitgestellt, die für die Installation und Verwendung der Host Intrusion Prevention 8.0-Software in einer verwalteten Umgebung erforderlich sind. Die Produkterweiterung wird auf den Versionen 4.0, 4.5 und 4.6 des ePolicy Orchestrator-Servers installiert. Der Client wird auf Windows-Workstations und -Servern sowie auf Solaris- und Linux-Servern installiert.

Produktfunktionen

Host Intrusion Prevention bietet eine zustandsorientierte Endpunkt-Firewall für Windows-Systeme und eine verwaltbare und skalierbare Intrusionspräventionslösung für Arbeitsstationen, Notebooks und unternehmenskritische Server (einschließlich Web- und Datenbankservern) unter Windows und anderen Betriebssystemen. Mit Host Intrusion Prevention wird unerwünschter oder gefährlicher Netzwerkverkehr blockiert. Außerdem können Zero-Day- und sonstige bekannte Angriffe mit patentierter und preisgekrönter Technologie proaktiv blockiert werden. Es sind zwei Versionen von Host Intrusion Prevention 8.0 verfügbar: eine reine Firewall-Version und eine vollständige Version mit Firewall- und IPS-Schutz.

Verwaltbarkeit und Skalierbarkeit

Der ePolicy Orchestrator verwaltet die Host Intrusion Prevention und ermöglicht die Nutzung und Durchsetzung der Programmrichtlinien zusammen mit anderen kritischen Sicherheitslösungen wie dem Virenschutz. Dieser verwaltete Ansatz erhöht die Kommunikation zwischen Anwendungen und bietet eine umfassende Lösung, die die unternehmensweite Bereitstellung auf bis zu 100.000 Clientsystemen in mehreren Sprachen möglich macht und so eine umfassende, globale Abdeckung bietet.

Sicherheit

Host Intrusion Prevention kombiniert Verhaltensregeln, Signaturen und eine statusbehaftete System-Firewall für die Blockierung von Angriffen und die Verringerung der Notwendigkeit, neue Patches zum Schutz vor neuen Bedrohungen zu installieren. Sie sind durch die Standardeinstellungen abgesichert, die eine schnelle Bereitstellung auf einer Vielzahl an Computern erlauben. Für noch höheren Schutz haben Sie die Möglichkeit, strengere vordefinierte oder benutzerdefinierte Richtlinien anzuwenden.

Die ePO-Datenbank enthält Sicherheitsinhaltsdaten, einschließlich Signaturen, die in den Host Intrusion Prevention-Richtlinien angezeigt werden. Aktualisierungen erfolgen über ein Inhaltsupdate-Paket, das Versionsinformationen und Skript-Aktualisierungen enthält. Beim Einchecken wird die Paketversion mit den aktuellsten Inhaltsinformationen in der Datenbank verglichen. Wenn das Paket neuer ist, werden die Inhaltsdaten extrahiert und gespeichert.

Diese neuen Inhaltsinformationen werden anschließend bei der nächsten Agent-zu-Server-Kommunikation an Clients weitergeleitet.

HINWEIS: Inhaltsupdates für Host Intrusion Prevention werden manuell oder automatisch mit einem Pull-Task in das ePO-Repository eingecheckt und mit einem Aktualisierungstask an die Clients verteilt. Die Host Intrusion Prevention-Clients erhalten Aktualisierungen ausschließlich durch die Kommunikation mit dem ePO-Server.

So funktioniert der Schutz:

Der ePolicy Orchestrator überträgt Richtlinieninformationen in regelmäßigen Zeitabständen über den ePO-Agenten an Host Intrusion Prevention-Clients. Die Host Intrusion Prevention-Clients setzen die Richtlinien durch, sammeln Ereignisinformationen und übertragen diese Informationen über McAfee Agent zurück an ePolicy Orchestrator.

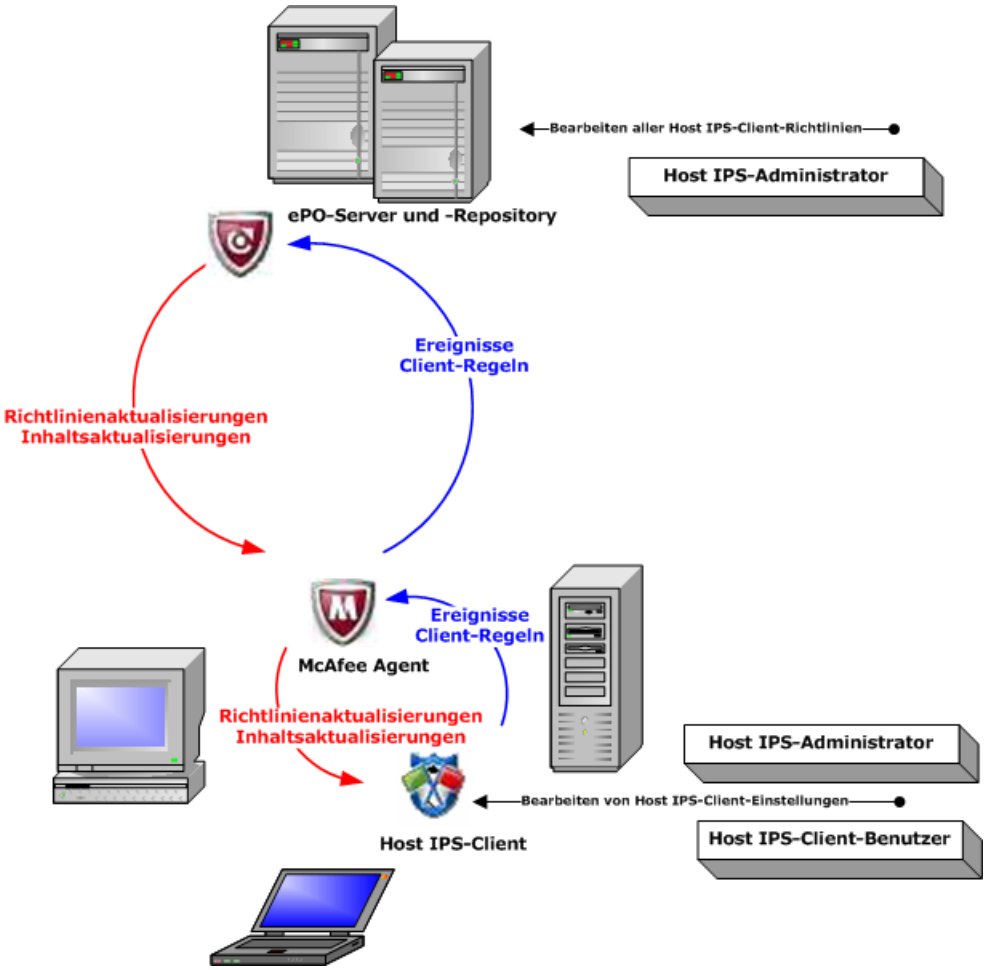

Abbildung 1: Schutz durch Host Intrusion Prevention

Inhalt

- Komponenten
- Installationsübersicht
- Neuheiten in dieser Version

Komponenten

Für die Host Intrusion Prevention-Software müssen verschiedene Komponenten installiert sein und ausgeführt werden, um Schutz zu gewährleisten:

Host Intrusion Prevention-Komponenten:

- ePolicy Orchestrator-Server und -Repository – das Verwaltungstool zur Installation von Client-Software, Übertragung neuer Richtlinien, Überwachung von Client-Aktivitäten, Erstellung von Berichten sowie Speicherung und Verteilen von Inhalts- und Client-Aktualisierungen.
- McAfee Agent – der auf einem verwalteten System installierte Server-Agent, der als Mittler zwischen dem Host Intrusion Prevention-Client sowie ePolicy Orchestrator-Server und -Datenbank fungiert. Er sendet Daten vom ePO-Server an den -Client und umgekehrt.
- Host Intrusion Prevention-Erweiterungen – die Schnittstelle für die Richtlinienverwaltung in der ePolicy Orchestrator-Konsole.
- Host Intrusion Prevention-Client – Hauptsoftwarekomponente, die Intrusionsschutz auf der Arbeitsstation oder dem Server bietet, auf dem er installiert ist.
- Host Intrusion Prevention-Inhaltsaktualisierungen (nur IPS-Schutz) – aktualisierte Sicherheitsinhalte, einschließlich Signaturen und vertrauenswürdigen Anwendungen, die in regelmäßigen Zeitabständen übertragen werden, um den Intrusionsschutz auf dem aktuellen Stand zu halten.

Installationsübersicht

Host Intrusion Prevention wird nur in einer ePolicy Orchestrator-Umgebung installiert. Ein ePO-Server und eine ePO-Datenbank müssen einsatzbereit sein, und auf jedem Client-System, auf dem Host Intrusion Prevention installiert werden soll, muss McAfee Agent installiert sein. Einzelheiten zu Anforderungen und Anleitungen zur Einrichtung dieser ePO-Umgebung finden Sie im Installationshandbuch von ePolicy Orchestrator.

Sobald ePO-Server und -Agenten eingerichtet sind, installieren Sie die entsprechende Host Intrusion Prevention-Erweiterung in ePO. Durch die von Ihnen erworbene Version des Produkts (nur Firewall-Schutz oder Firewall- und IPS-Schutz) und die von Ihnen verwendete ePO-Version wird bestimmt, welche Erweiterungen installiert werden müssen. Detaillierte Informationen finden Sie unter Installieren von ePolicy Orchestrator.

Als letzten Schritt installieren Sie Host Intrusion Prevention auf den Client-Computern unter Windows, Linux oder Solaris, auf denen bereits eine Version von McAfee Agent installiert ist. Detaillierte Informationen finden Sie unter Installieren des Windows-Clients. Installieren des Solaris-Clients bzw. Installieren des Linux-Clients.

HINWEIS: Die Firewall-Funktion von Host Intrusion Prevention gilt nur für Windows-Plattformen.

Auf Grund von Architekturänderungen in dieser Version werden Host Intrusion Prevention 8.0-Clients nur von der Host Intrusion Prevention 8.0-Erweiterung verwaltet. Sie können jedoch die Erweiterung von Version 7.0 neben der Erweiterung von Version 8.0 beibehalten und frühere

Client-Versionen verwalten, bis Sie für die Migration zu einer Umgebung von Version 8.0 bereit sind. Detaillierte Informationen zur Migration finden Sie unter Migrieren von Richtlinien.

Tabelle 1: Komponentenversionen

Auf dem ePolicy Orchestrator-Server		**Auf den Client-Systemen**		
Version	**Host IPS 8.0-Erweiterungen**	**Windows**	**Solaris**	**Linux**
4.0 Patch 6 und höher	Nur Firewall für ePO 4.0	• McAfee Agent 4.0 (Patch 3 und höher) oder McAfee Agent 4.5 (Patch 1 und höher) für Windows • Host IPS 8.0-Client	–	–
	Firewall und IPS für ePO 4.0	• McAfee Agent 4.0 (Patch 3 und höher) oder McAfee Agent 4.5 (Patch 1 und höher) für Windows • Host IPS 8.0-Client	• McAfee Agent 4.0 (Patch 3 und höher) oder McAfee Agent 4.5 (Patch 1 und höher) für Solaris • Host IPS 8.0-Client	• McAfee Agent 4.0 (Patch 3 und höher) oder McAfee Agent 4.5 (Patch 1 und höher) für Linux • Host IPS 8.0-Client
4.5	Nur Firewall für ePO 4.5	• McAfee Agent 4.0 (Patch 3 und höher) oder McAfee Agent 4.5 (Patch 1 und höher) für Windows • Host IPS 8.0-Client	–	–
	Firewall und IPS für ePO 4.5	• McAfee Agent 4.0 (Patch 3 und höher) oder McAfee Agent 4.5 (Patch 1 und höher) für Windows • Host IPS 8.0-Client	• McAfee Agent 4.0 (Patch 3 und höher) oder McAfee Agent 4.5 (Patch 1 und höher) für Solaris • Host IPS 8.0-Client	• McAfee Agent 4.0 (Patch 3 und höher) oder McAfee Agent 4.5 (Patch 1 und höher) für Linux • Host IPS 8.0-Client
4.6	Nur Firewall für ePO 4.6	• McAfee Agent 4.0 (Patch 3 und höher) oder McAfee Agent 4.5 (Patch 1 und höher) für Windows • Host IPS 8.0-Client	–	–
	Firewall und IPS für ePO 4.6	• McAfee Agent 4.0 (Patch 3 und höher) oder McAfee Agent 4.5 (Patch 1 und höher) für Windows • Host IPS 8.0-Client	• McAfee Agent 4.0 (Patch 3 und höher) oder McAfee Agent 4.5 (Patch 1 und höher) für Solaris • Host IPS 8.0-Client	• McAfee Agent 4.0 (Patch 3 und höher) oder McAfee Agent 4.5 (Patch 1 und höher) für Linux • Host IPS 8.0-Client

Neuheiten in dieser Version

Diese Version des Produkts umfasst verschiedene neue Funktionen, Verbesserungen und Änderungen.

IPS

- Neue Funktionen für die Richtlinie zu den IPS-Optionen:
  - Schutz bei Systemstart: Schutz bei Systemstart, bevor die IPS-Dienste gestartet werden
- Neue Funktion für die Richtlinie zu den IPS-Regeln:
  - Auf der IP-Adresse für Netzwerk-IPS-Signaturen basierende Ausnahmen
  - Vertrauenswürdige Netzwerke für IPS-Signaturen und Firewall-Regeln
  - Die Übereinstimmung ausführbarer Dateien für Anwendungen wird bei Signaturen und Ausnahmen nun nach Pfad, Hash, digitaler Signatur und Dateibeschreibung und nicht nur nach Pfad vorgenommen.

Firewall

- Neue Funktionen für die Richtlinie für Firewall-Optionen:
  - TrustedSource-Bewertung und -Blockierung: Firewall-Regeln blockieren oder erlauben eingehenden oder ausgehenden Verkehr entsprechend den McAfee TrustedSource-Bewertungen.
  - IP-Fälschungsschutz: Firewall-Regeln blockieren ausgehenden Verkehr, wenn es sich bei der lokalen IP-Adresse nicht um eine IP-Adresse des lokalen Systems handelt und wenn die lokale MAC-Adresse keine MAC-Adresse eines VM-Gasts ist.
  - Bridged-VM-Unterstützung: Firewall-Regeln lassen Verkehr über eine lokale MAC-Adresse zu, bei der es sich nicht um die MAC-Adresse des lokalen Systems handelt, sondern um eine der MAC-Adressen im Bereich der unterstützten VM-Software.
  - Schutz bei Systemstart: Firewall-Regeln blockieren den gesamten eingehenden Verkehr, bevor die Firewall-Dienste gestartet werden.
- Zusätzliche Firewall-Richtlinie: Firewall-DNS-Blockierung, die aus einer Reihe zu blockierender Domänennamenmuster besteht. Mit dieser Richtlinie wird die Domänenregel ersetzt, die die DNS-Auflösung für vom Benutzer angegebene Domänennamen blockiert hat.
- Neue Funktionen für die Richtlinie für Firewall-Regeln:
  - Firewall-Regeln sind viel flexibler: Eine einzelne Regel kann nun mehrere Anwendungen (früher nur eine), mehrere Netzwerke (früher nur eines), ein lokales Netzwerk und ein Remote-Netzwerk (früher nur ein Remote-Netzwerk) und zusätzlich zu drahtgebundenen und drahtlosen Medientypen auch einen VPN-Medientyp umfassen.
  - Bei Verbindungsgruppen (CAG, Connection-Aware Group) handelt es sich nun einfach um Firewall-Gruppen, die über Standortinformationen und Zeitpläne mit zeitbasiertem Zugriff auf ihnen zugeordnete Verbindungen verfügen.
  - Die Übereinstimmung ausführbarer Dateien für Anwendungen wird bei Firewall-Regeln nun nach Pfad, Hash, digitaler Signatur und Dateibeschreibung und nicht nur nach Pfad und Hash vorgenommen.

Allgemein

- Die Richtlinien für Anwendungsblockieroptionen und Anwendungsblockierregeln wurden entfernt, und ihre Funktionalität wurde durch zwei Inhaltssignaturen (6010 und 6011) in der Richtlinien für Host IPS-Regeln ersetzt.
- Die Richtlinien für Firewall-Quarantäne-Optionen und Quarantäne-Regeln wurden entfernt, und die Systemstart-Quarantäne-Option wurde in eine Option zum Schutz bei Systemstart in den Firewall-Optionen verschoben.
- Neuer Host IPS-Katalog zum Organisieren und Ermöglichen der erneuten Verwendung häufig verwendeter Richtlinienkomponenten für Richtlinien, insbesondere Firewall-Gruppen, Regeln, Standort, ausführbare Dateien und Netzwerke.
- Einzelne im gesamten Produkt verwendete Standardplatzhalter
- In einem allgemeinen Ordner gespeicherte Protokolle, von denen einige für eine einfache Lesbarkeit vereinfacht wurden

Unterstützte Plattformen

- Vollständige Funktionsparität für Windows-Plattformen mit 32-Bit und 64-Bit
- Hinzugefügt: Unterstützung von Windows 7, Linux SUSe10 SP3, SUSe 11, Solaris Zone
- Entfernt: Windows 2000, Solaris 8 und SUSe Linux 9

SQL-Unterstützung

- Hinzugefügt: SQL 2005, SQL 2008
- Entfernt: SQL Server 2000

Erweiterungs-/Client-Funktionalität

- Zwei Versionen von Host Intrusion Prevention 8.0: eine reine Firewall-Version und eine vollständige Version mit Firewall- und IPS-Schutz.
- Host IPS-Erweiterungskompatibilität mit den Versionen 4.0, 4.5 und 4.6 von ePolicy Orchestrator.
- Möglichkeit zum Installieren der Host IPS 8.0-Erweiterung in ePolicy Orchestrator, selbst wenn frühere Versionen von Host IPS installiert sind.
- Die Host IPS 8.0-Erweiterung verwaltet nur Host IPS 8.-Clients. Frühere Client-Versionen können nicht unterstützt werden.
- Der IPS- und Firewall-Schutz wird nach der ersten Installation auf dem Client deaktiviert und muss von der Anwendung einer Richtlinie aktiviert werden.
- Auf allen Plattformen kann die Aktualisierung von der Testversion auf die lizenzierte Version von ePolicy Orchestrator ohne erneute Installation eines Clients vorgenommen werden.

Bewährte Vorgehensweisen für einen einfachen Weg zum Erfolg

McAfee Host Intrusion Prevention bietet Ihrem Unternehmen einen hohen Wert: durch die Senkung der Häufigkeit und Dringlichkeit der Installation von Patches, die Gewährleistung von Geschäftsbetrieb und Mitarbeiterproduktivität, den Schutz der Vertraulichkeit von Daten und Unterstützung für die Vorschriften-Compliance. Es bietet ein signatur- und verhaltensorientiertes Eindringungsschutzsystem (IPS, Intrusion Prevention System) und eine zustandsorientierte Firewall, um sämtliche Endpunkte (Desktop-Computer, Laptops und Server) vor bekannten und unbekannten Bedrohungen zu schützen.

Erste Schritte

Alle Elemente, die Benutzer und geschäftsrelevante Anwendungen betreffen, müssen unter Wahrung der Sorgfalt ausgebracht werden, um Störungen der Geschäftstätigkeit zu verhindern. In diesem Abschnitt wird ein Rollout des Produkts erläutert, das in kleine, leicht zu bewältigende Stufen aufgeschlüsselt ist. So können der Schutz vorsichtig erhöht, Richtlinien genau auf die Unterstützung für geschäftsbezogene Besonderheiten abgestimmt und die Veränderungen für die Benutzer klein gehalten werden. Dieser schrittweise, aber kontinuierliche Vorgang bietet maximalen Schutz bei minimalem Verwaltungsaufwand und erstreckt sich über einen bis drei Monate.

Wenn Sie IPS und Firewall-Schutz erworben haben, wird empfohlen, mit der IPS-Funktion zu beginnen, sofern die Firewall aufgrund gesetzlicher Vorschriften oder risikobezogener Erwägungen für Sie nicht von vorrangiger Bedeutung ist. Die IPS-Funktion umfasst entscheidenden, universell erforderlichen Schutz gegen bekannte Risiken und Zero-Day-Bedrohungen. Sie können McAfee Host Intrusion Prevention mit den vordefinierten Richtlinieneinstellungen von McAfee und nur geringem Zeitaufwand schnell einrichten und so Systeme gegen Schwachstellen und Angriffe schützen.

Nach der Aktivierung des IPS-Schutzes können Sie dann die Aktivierung der Firewall vornehmen. Die hier beschriebene Einführungsstrategie gilt für das Firewall-Rollout. Die konkreten Richtlinien, Reaktionen und Regeln sind jedoch fallabhängig.

HINWEIS: Verwenden Sie die hier beschriebene Strategie, wenn Sie nur den Firewall-Schutz erworben haben oder die Firewall einfach zuerst ausbringen möchten. Details zur Definition und Aktivierung von Firewall-Richtlinien können Sie dem Produkthandbuch oder der Hilfe entnehmen. Der zentrale Gedanke besteht darin, das Rollout in Stufen auszuführen. Empfohlen wird diese Reihenfolge:

- IPS auf Laptops und Standard-Desktop-Computern
- IPS auf unternehmenskritischen Servern
- IPS auf Laptops und Desktop-Computern von Hauptbenutzern
- Firewalls auf Laptops
- Firewalls auf Servern
- Firewall auf Laptops und Desktop-Computern von Hauptbenutzern

Die meisten Administratoren können die hier genannten Schritte ausführen. Bei Bedarf können Sie auch Unterstützung durch McAfee-Partner und Service-Mitarbeiter erhalten.

Die empfohlene Abfolge umfasst sieben Schritte:

1. Strategie und Planung
2. Vorbereiten der Umgebung
3. Installation und Konfiguration
4. Grundanpassung
5. Optionaler adaptiver Modus
6. Erweiterter Schutz und erweiterte Anpassung
7. Wartung und Erweiterung über IPS hinaus

Der Rollout-Prozess ist für Desktop-Computer und Server ähnlich. Es ist jedoch zu empfehlen, den Schutz zunächst an konservativeren Punkten einzurichten und für komplexere und unternehmenskritische Desktop-Computer von Hauptbenutzern und Server in Phasen aufzubauen.

Zeitplanung und Erwartungen

Bei einem erfolgreichen Rollout mit minimalen Komplikationen und maximaler Risikominimierung dauert der Einführungsprozess einen bis drei Monate. Die eigentlichen Arbeiten beanspruchen in diesem Zeitraum nur einige Tage. Zwischen den einzelnen Stufen muss jedoch Zeit verstreichen, damit vom Produkt die Verwendungsdaten erfasst werden können, die für die Anpassung erforderlich sind.

Die Hauptvariable bei der Implementierung ist der Umfang an Systemen und Benutzerprofilen am Standort. Je breiter die Benutzergruppe gefächert ist, desto länger dauert es, McAfee Host Intrusion Prevention auf allen ausgewählten Systemen zu implementieren. Die Schutzoptionen müssen aktiviert werden, ohne die Produktivität der Benutzer und die Funktionsfähigkeit von Anwendungen zu beeinträchtigen. Für jedes wichtige System und Benutzerprofil sollten Anpassungen und Tests durchgeführt werden.

In vielen Umgebungen müssen die Ausbringung, die Migration auf den Blockiermodus und die Verwendung der Firewall vom IT-Management genehmigt werden. Kalkulieren Sie für diese Genehmigungen eine Zeitreserve ein.

HINWEIS: Einzelheiten zu den Aspekten dieses Prozesses finden Sie im *Host Intrusion Prevention 8.0-Produkthandbuch*.

Tabelle 2: Mögliche Schwierigkeiten und Lösungen

Diese Dinge sollten Sie unbedingt vermeiden	Empfohlene bewährte Vorgehensweisen
Signaturen mittleren und hohen Schweregrads blockieren, ohne zunächst das Protokoll zu prüfen.	Blockieren Sie zunächst nur Signaturen mit hohem Schweregrad. Bei dieser Stufe besteht Schutz an den wichtigsten Schwachstellen, und es werden nur wenige Fehlereignisse ausgelöst. Signaturen mittleren Schweregrads beziehen sich auf Verhaltensweisen und setzen zumindest eine gewisse Anpassung voraus, um die Zahl der Support-Anrufe zu begrenzen.
Davon ausgehen, dass für alle Systeme dieselben Richtlinien verwendet werden.	Teilen Sie Desktop-Computer nach Anwendungen und Rechten in Gruppen auf. Beginnen Sie mit den einfachsten Systemen, und erstellen Sie für große Gruppen Standardnutzungsprofile. Fügen Sie schrittweise weitere Benutzer und Nutzungsprofile in dem Maß hinzu, in dem Sie Erfahrung gewinnen.
Unzureichend auf Benutzerfreundlichkeit testen.	Wählen Sie einige wichtige Benutzergruppen aus, führen Sie Tests mit Pilotbenutzern aus, die Feedback einbringen, prüfen Sie, ob Anwendungen weiterhin richtig

Diese Dinge sollten Sie unbedingt vermeiden	Empfohlene bewährte Vorgehensweisen
	funktionieren, und setzen Sie dann ein breit angelegtes Rollout um, wenn die Richtlinien erwiesenermaßen funktionieren, ohne die Produktivität zu stören. Bemühen Sie sich darum, bei den Benutzern einen guten ersten Eindruck zu hinterlassen.
Host IPS einrichten und dann zu den Akten legen.	Anders als bei Antivirus-Lösungen sind regelmäßige Überwachung und Wartung erforderlich, um die Genauigkeit und Wirksamkeit des Schutzes zu gewährleisten. Planen Sie nach Abschluss der Ausbringung Zeit für die (mindestens wöchentliche) Durchsicht von Protokollen und die Aktualisierung von Regeln ein.
IPS und Firewall gleichzeitig aktivieren.	Beginnen Sie mit IPS und fügen Sie die Firewall je nach Bedarf hinzu. Sie wissen dann bereits, wie Richtlinien erstellt werden, haben sich mit den jeweils geeigneten Arten von Schutz vertraut gemacht und können Änderungen und Ergebnisse besser in Beziehung zueinander setzen.
Host IPS- oder Firewall-Funktionen für unbestimmte Zeit im adaptiven Modus belassen.	Verwenden Sie den adaptiven Modus für kurze Zeitabschnitte, wenn es ihnen möglich ist, die erstellten Regeln zu überwachen.
Alles, was vom System an Eindringversuchen entdeckt wird, sofort blockieren.	Nehmen Sie sich die Zeit, zu überprüfen, ob der angezeigte Datenverkehr tatsächlich eine Bedrohung darstellt. Verwenden Sie dafür Paketaufzeichnung, Netzwerk-IPS und sonstige Methoden.

- 1. Entwickeln einer Strategie
- 2. Vorbereiten einer Pilotumgebung
- 3. Installieren und Konfigurieren
- 4. Grundanpassung
- 5. Aktivieren des adaptiven Modus (optional)
- 6. Feinabstimmung
- 7. Ausführen der Wartung und Erweiterung

1. Entwickeln einer Strategie

Der erste Schritt im Abstimmungsprozess besteht darin, über die Strategie für den Systemschutz nachzudenken. Legen Sie realistische Ziele fest, und erstellen Sie einen entsprechenden Pilot- und Bereitstellungsplan.

Definieren der Prioritäten des Pilots

Stellen Sie sicher, dass Sie Ihre Ziele hinsichtlich der Sicherheit verstehen, und richten Sie den Pilotprozess entsprechend aus. Möglicherweise möchten Sie einige bestimmte Probleme identifizieren, die sofort blockiert werden sollen, oder einen allgemeinen Überwachungszeitraum festlegen, um mehr darüber zu erfahren, was wirklich in der Client-Community geschieht. Jede Organisation beurteilt das Verhältnis zwischen Schutz und Produktivität unterschiedlich. Durch klare Prioritäten am Anfang wird der Prozess optimiert.

Stellen Sie sich diese Fragen:

- Welche speziellen Sicherheitsschwachstellen gibt es, oder auf welche Vorfälle wurde in Audits verwiesen?

- Welche Systeme sind am stärksten gefährdet?
- Haben mobile Laptops eine Priorität?
- Muss ich laut Vorschriften die Gefährdung in einer wichtigen Benutzer-Community oder Systemgruppe reduzieren?

Für die meisten Kunden stellen Laptops, die die kontrollierte Unternehmensumgebung verlassen, die größte Gefährdung dar. Diese Systeme stellen hervorragende erste Ziele für IPS dar. Einige Kunden möchten den Schutz wichtiger Server verstärken. Es wird empfohlen, diese unternehmenskritischen Systeme erst später in die Pilotumgebung aufzunehmen. Notieren Sie Ihre wichtigsten Ziele. Die nächsten wenigen Schritte werden Ihnen bei der Priorisierung helfen.

Definieren der Pilotumgebung

Wählen Sie eine kleine Gruppe von Pilotsystemen aus, auf denen eine Testanpassung ausgeführt wird. Indem Sie maximal 100 Knoten in drei Subnetzen auswählen, können Sie schrittweise von den anfänglichen konventionellen Schutzstufen zum neuen Schutz wechseln. Bei einer schrittweisen Erweiterung können Sie sofort auf Probleme reagieren, sobald sie auftreten.

Differenzieren Sie die Hauptarten der Systeme, und schließen Sie sie selektiv in Ihren Pilot ein. Von der geringsten bis zur höchsten Implementierungkomplexität kann Host IPS Folgendes unterstützen:

- Standardisierte Desktops oder Laptops, für die durchschnittliche Benutzer nicht über Administratorrechte zum Installieren oder Löschen von Anwendungen auf ihren Systemen verfügen. Sie können mehrere Benutzerprofile erstellen, von denen jedes eine definierte Standardanwendungsumgebung aufweist.
- Angepasste Hauptbenutzer-Desktops oder -Laptops, für die spezialisierte Benutzer über Administratorrechte zum Installieren eigener Anwendungen verfügen. Zu den Hauptbenutzern gehören in der Regel Administratoren und Softwareentwickler. Gelegentlich werden Administratorrechte als Geschäftsgegenstand angesehen. Im Idealfall sollten diese Rechte auf Systemen, für die keine Administratorkontrolle erforderlich ist, entfernt werden, um den Bereich von Systemtypen zu reduzieren, für den Profile erstellt und Abstimmungen vorgenommen werden müssen.
- Server, auf denen dedizierte Datenbank-, Web-, E-Mail-Anwendungen und andere Anwendungen ausgeführt werden sowie Druck- und Dateiserver.

Labor oder reale Welt?

In vielen Unternehmen sind Labortests als Standardschritt bei der Installation neuer Produkte erforderlich. Sie erstellen Abbilder von Produktionssystemen und testen die Abbilder vor dem Rollout in einer kontrollierten Umgebung.

Mit McAfee Host Intrusion Prevention bietet diese Methode die schnellste Grundlage an Regeln, aber es ist der ineffektivste Gesamtvorgang, da die Benutzervariable ausgelassen wird. Tester stellen das Benutzerverhalten künstlich nach. Daher ist es unwahrscheinlich, dass sie authentische Einzelheiten zu berechtigten Aktivitäten erfassen. Benutzer und Malware finden immer neue Verwendungsmöglichkeiten, mit denen Ereignisse erzeugt werden, die unmittelbar geprüft werden müssen oder deren Erkennung umgangen wird, wenn sie unwissentlich als Ausnahme zum "normalen Verhalten" zugelassen wurden. Beide Fälle kosten Zeit und können später zu Problemen führen.

Die meisten Lernerfolge werden bei realen Systemen in einer Produktionsumgebung erzielt. Bei den besten Produktionstests werden sorgfältig ausgewählte Systeme und objektive Benutzer verwendet, die alltägliche Aufgaben ausführen. Diese Methode bietet die zuverlässigste Basis, da reale Benutzer ihre Systeme und Anwendungen ändern. Sie können sofort Feedback zu den Auswirkungen der Änderungen geben.

Die Kombination beider Modelle stellt eine gute Lösung dar. Ein Labortest schafft Vertrauen und lässt Sie mit den Prozessen und Richtlinien von McAfee Host Intrusion Prevention vertraut werden. Nachdem einige Benutzungsprofile gestestet wurden, können diese Profile in einen Pilot auf Produktionssystemen verschoben werden. Aktivitäten oder Anwendungen, die im Labortest ausgelassen wurden, können dann im Produktionspilot berücksichtigt werden. Dieser aus zwei Schritten bestehende Prozess eignet sich sehr für konservative Unternehmen.

TIPP: Administratoren müssen über einfachen physikalischen Zugriff auf Pilotsysteme verfügen. Das bedeutet, dass unbesetzte Büros und Privatanwender aus der ersten Pilotgruppe ausscheiden.

Sicherstellen einer entsprechenden Benutzerdarstellung

Mit den Kenntnissen hinsichtlich der Systemtypen müssen Sie zunächst die Verwendungsprofile und Systeme im Pilot identifizieren. Schließen Sie unterschiedliche Benutzertypen ein, um einen Querschnitt der möglichen Zielbenutzer-Community zu erhalten. Auf diese Weise können Sie Regeln und Richtlinien erstellen, die die normalen Unternehmensanforderungen und -verwendungen widerspiegeln. In einem standardisierten Callcenter-Call oder Helpdesk gibt es beispielsweise Manager, Kundensupport und Händlersupport. Stellen Sie sicher, dass Sie mindestens eines der jeweiligen Benutzungsprofile einschließen, damit von McAfee Host Intrusion Prevention Richtlinien für das gesamte Verwendungsspektrum ermittelt und erstellt werden.

Rollout-Strategie 1: Einfach starten

Für eine schnelle Implementierung des anfänglichen Schutzes und eine möglichst aufwandsfreie Lernkurve hin zum erweiterten Schutz wird die Aktivierung des Basisschutzes auf standardisierten Desktops und Laptops sowie die Aktivierung der Protokollierung auf den Hauptbenutzer-Desktops und -Servern empfohlen.

Aktivieren Sie zunächst den Schutz, indem Sie die Richtlinie **IPS-Optionen** mit ausgewähltem IPS-Schutz anwenden, und wenden Sie dann die Basisrichtlinie **McAfee-Standard-IPS-Regeln** an. Diese Richtlinie blockiert Aktivitäten, die Signaturen mit hohem Schweregrad auslösen, keine Abstimmung erfordern und wenig Ereignisse generieren. Ihre Einstellungen umfassen:

- Aktivitäten, die Signaturen mit hohem Schweregrad auslösen, werden blockiert, und alle anderen Signaturen werden ignoriert.
- McAfee-Anwendungen werden für alle Regeln außer den IPS-Selbstschutzregeln als vertrauenswürdige Anwendungen aufgeführt. Als vertrauenswürdige Anwendungen generieren sie beim Verwenden keine Ausnahmeereignisse.
- Vordefinierte Anwendungen und Prozesse werden geschützt.

Obwohl die Fabrikate und Modelle von Computern unterschiedlich sind, liegen diese Unterschiede jedoch relativ nah beieinander. Auf Grund umfangreicher Erfahrungen können die Probleme mit einem hohen Schweregrad durch die IPS-Funktion mit hoher Genauigkeit abgedeckt werden. McAfee hat beispielsweise aufgezeigt, dass 90 Prozent oder mehr der Probleme des "Patch-Dienstags" von Microsoft mithilfe der sofort einsatzbereiten Basisschutzstufe abgeschirmt wurden. Selbst das Aktivieren des Standardschutzes bietet einen beträchtlichen sofortigen Wert.

Die Strategie des einfachen Starts wird dringend empfohlen. Server sind möglicherweise die wichtigsten Systeme, die geschützt werden müssen, aber sie stellen wahrscheinlich auch die schwierigsten Systeme dar. Sie erfordern mehr Aufmerksamkeit bei der Bereitstellung, da IPS-Regeln zwangsläufig so angepasst werden müssen, dass legitime Anwendungsvorgänge zugelassen werden und die sorgfältige Leistungs- und Systemoptimierung auf den meisten Servern widergespiegelt wird. Das Abstimmen von Regeln nach der Methode Versuch und Irrtum kann auf realen und unternehmenskritischen Systemen gefährlich sein.

Ebenso verfügen Hauptbenutzersysteme meist über unterschiedliche Anwendungen und spezielle Rechte wie das Recht zum Ausführen von Skripts. Durch das Aktivieren von IPS kann eine

Vielzahl von Ereignissen erzeugt werden, die genau überprüft werden müssen, um entsprechende Berechtigungen oder Blockierungen zuzulassen. Hauptbenutzer und Server benötigen mehr Zeit zum Nachvollziehen der legitimen Verwendung.

Überwachung und Protokollierung

Da das Vertrauen während der Pilotphase wächst, können Sie Signaturen von der Protokollierung zur aktiven Erzwingung nach Systemklasse, Abstimmungsregeln und Verfeinerungsrichtlinien verschieben, indem Sie lernen, welche Aktivitäten legitim sind. Dieser Prozess wird weiter hinten in diesem Handbuch beschrieben.

Während Sie den Standardschutz auf Ihren standardmäßigen Desktop-Systemen aktivieren, können Sie auch die Protokollierung von Problemen mit mittlerem Schweregrad auf dem System initiieren. Mit dieser Überwachung können Sie andere Ereignisse ermitteln, die von der IPS-Funktion gekennzeichnet werden, wenn Sie mit dem engeren Blockieren von Steuerelementen beginnen. Im Protokollierungsmodus sehen Sie den Verwendungsanteil sowie die Verwendungstypen, damit Sie mehr über das Systemverhalten erfahren können. Die Protokollierung wird in dieser ersten Phase empfohlen, um böse Überraschungen und Störungen zu vermeiden. Ereignisse sollten für einen vollständigen Geschäftszeitraum (mindestens einen Monat und vielleicht ein gesamtes Quartal) protokolliert werden, um das gesamte Ausmaß von Anwendungen und Aktivitäten zu sehen. Verwenden Sie die Richtlinie **Erweiterten Schutz vorbereiten**, um Ereignisse automatisch zu protokollieren. Mit dieser Einstellung werden Signaturen mit hohem Schweregrad vermieden und Signaturen mit mittlerem Schweregrad protokolliert; der Rest wird ignoriert.

Legen Sie auf Ihren anderen Systemen, Servern und Hauptbenutzer-Desktops die Überwachung und Protokollierung für mittlere und hohe Sicherheitsstufen fest. Es gibt keine Standardeinstellung, mit der mittlere und hohe Stufen protokolliert werden. Daher müssen Sie eine vorhandene Richtlinie duplizieren und anpassen. Das reine Überwachen von Ereignissen der mittleren und hohen Sicherheit bietet ein gutes Maß an relevanten Informationen, ohne Sie mit Details zu überfluten. Sie entdecken die Systemunterschiede, bei denen Serverplattformen auf jede bestimmte Anwendungsinstanz abgestimmt sind oder für die Entwickler ihre Lieblingstools und geheimen Compiler haben.

TIPP: Die Aktivierung der Überwachung und Protokollierung sollte sich nicht auf System- oder Anwendungsvorgänge auswirken. Es ist jedoch immer ratsam, Systeme direkt nach der Bereitstellung von McAfee Host Intrusion Prevention zu überwachen, selbst wenn dies nur in einem reinen Protokollierungsmodus geschieht. Da das Produkt geringfügig mit Änderungen und Betriebssystemen interagiert, ist es immer möglich, dass es sich auf die Leistung einiger Anwendungen auswirkt.

Planen der Erweiterung

Da das Vertrauen während der Pilotphase wächst, können Sie Signaturen von der Protokollierung zur aktiven Erzwingung nach Systemklasse, Abstimmungsregeln und Verfeinerungsrichtlinien verschieben, indem Sie lernen, welche Aktivitäten legitim sind. Dieser Prozess wird weiter hinten in diesem Handbuch beschrieben.

Rollout-Strategie 2: Standardrichtlinien verwenden

Bei einigen Umgebungen ist es legitim, das Fachwissen von McAfee zu nutzen, das in den Standardeinstellungen steckt, und das Basisschutzprofil für alle Systeme zu verwenden. Diese Methode eignet sich für Benutzer, die den IPS-Grundschutz verwenden möchten, ohne viele Abstimmungen vorzunehmen oder großen Aufwand zu treiben. Wenn IPS nicht der Hauptgrund für den Erwerb des Produkts ist, bietet diese Strategie eine Bereitstellung mit minimalem Aufwand, die sofortigen Schutz vor den großen Angriffen bietet.

Auswählen der Strategie

Mit Strategie 1 können Sie vom besten Schutz Ihrer IPS-Investition profitieren. Strategie 2 stellt eine zuverlässige Strategie mit geringem Aufwand dar. Entscheiden Sie sich für die Strategie, die Ihrem Risiko, dem Sie ausgesetzt sind, am besten gerecht wird.

2. Vorbereiten einer Pilotumgebung

Nachdem Sie Ihre Prioritäten, Ziele und Schutzstrategie definiert haben, sollten Sie sicherstellen, dass Ihre Umgebung den technischen Voraussetzungen entspricht, und vor der Installation eventuelle Systemfehler beseitigen. Mit dieser Vorbereitungsarbeit können Sie sich auf die IPS-Bereitstellung konzentrieren und potentielle Probleme vermeiden, die nicht mit dieser Funktion in Verbindung stehen.

Installieren oder Aktualisieren von McAfee ePolicy Orchestrator und Agent

Vor dem Installieren von McAfee Host Intrusion Prevention muss zunächst der ePolicy Orchestrator-Server installiert werden, und Sie müssen McAfee Agent auf den Zielhosts installieren.

Sie müssen über Kenntnisse hinsichtlich der Richtlinienimplementierung mit ePolicy Orchestrator verfügen, um McAfee Host Intrusion Prevention erfolgreich anpassen zu können. Wenn Sie noch nicht mit der Richtlinienerstellung mithilfe von ePolicy Orchestrator vertraut sind, finden Sie in der Dokumentation zu ePolicy Orchestrator weitere Informationen.

Warum ePolicy Orchestrator?

Für McAfee Host Intrusion Prevention ist ePolicy Orchestrator erforderlich, da seine Bereitstellung auf organisationsspezifischen Richtlinien und Regeln beruht, die routinemäßig angepasst werden, wenn sich die Unternehmens- oder Benutzer-Community ändert. Von McAfee Host Intrusion Prevention werden die Vorteile der bewährten Infrastruktur von ePolicy Orchestrator genutzt, durch die die Konsistenz der Richtlinienanwendung erhöht, Fehler reduziert und die Sichtbarkeit und Kontrolle für Administratoren verbessert werden.

Prozessübersicht:

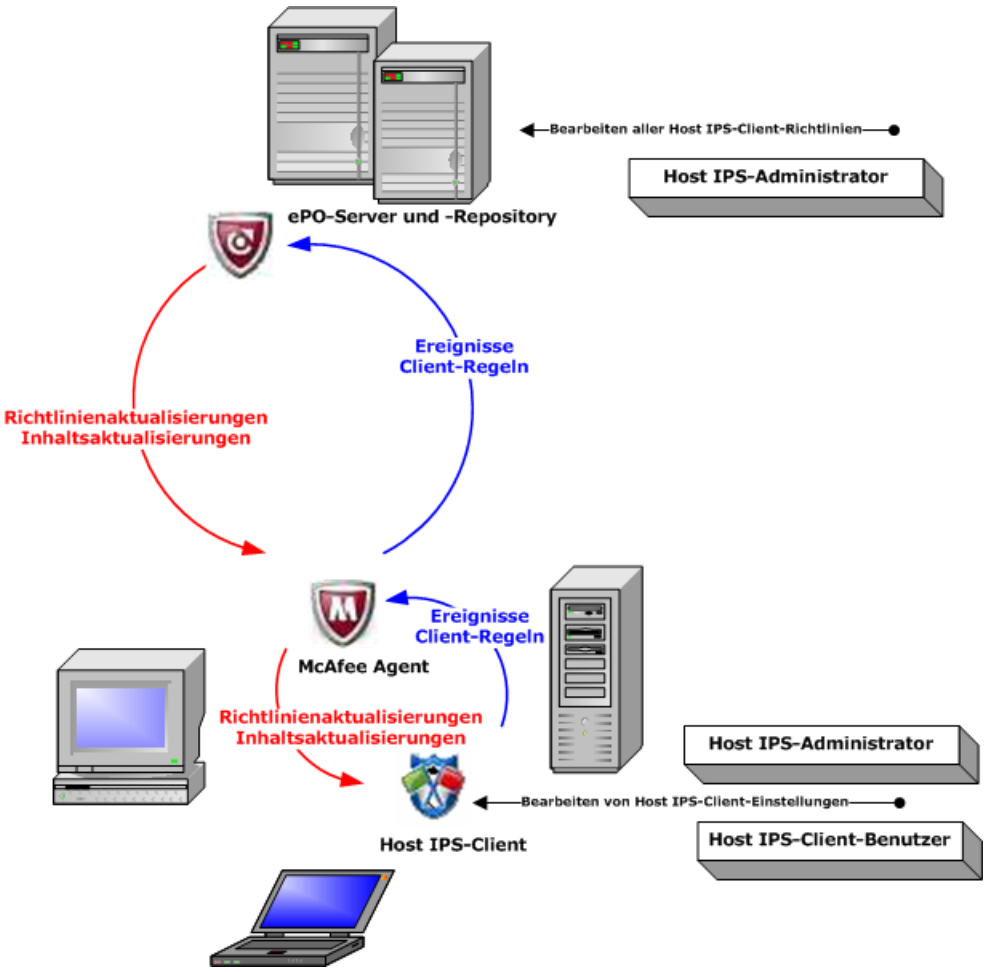

Abbildung 2: Host Intrusion Prevention-Installation und -Wartung mithilfe von ePolicy Orchestrator

- Vom ePO-Server wird auf jedem Server McAfee Agent verwendet, um den IPS-Client auf allen Zielsystemen zu installieren.
- IPS-Richtlinien werden mithilfe der ePO-Konsole erstellt und verwaltet.
- Der ePO-Server überträgt die Richtlinien an den Agenten auf dem Zielsystem.
- Der Agent überträgt die Richtlinien an den IPS-Client.
- Der IPS-Client erzwingt die Richtlinien und generiert Ereignisinformationen, die er an den Agenten sendet.
- Der Agent überträgt Ereignisinformationen zurück an ePolicy Orchestrator.
- In geplanten Intervallen oder auf Anforderung ruft der ePO-Server Inhalts- und Funktionalitätsaktualisierungen aus dem McAfee-Repository ab, und der Agent ruft sie vom Server ab, um den IPS-Client zu aktualisieren.
- Wenn Richtlinien geändert werden, werden Sie vom Agenten angerufen, um den IPS-Client zu aktualisieren.

Verwenden des ePO-Servers zum Einrichten von Verwendungsprofilen und Clients

Erstellen Sie für jeden unterschiedlichen Verwendungstyp (Web-Server, Laptops, Kiosks) ein unterschiedliches ePO-Verwendungsprofil. Sie weisen diesen Profilen letztlich IPS-Richtlinien zu. Es ist hilfreich, diese Profile vorab einzurichten, wenn Sie Ausnahmen verwalten müssen.

Gruppieren Sie die Clients logisch. Clients können nach beliebigen Kriterien gruppiert werden. Die Gruppierung muss allerdings zur Hierarchie der ePO-Systemstruktur passen. Sie können z. B. eine erste Ebene nach geografischem Standort und eine zweite Ebene nach Betriebssystemplattform oder nach IP-Adresse gruppieren. Es wird empfohlen, Systeme in Gruppen – basierend auf McAfee Host Intrusion Prevention-Konfigurationskriterien – anzuordnen, einschließlich des Systemtyps (Server oder Desktop), der wichtigen Anwendungen (Web-, Datenbank- oder E-Mail-Server) und der strategischen Positionen (DMZ oder Internet).

TIPP: Der ePO-Server lässt die logische Kennzeichnung von Systemen zu. Kennzeichnungen sind wie Beschriftungen, die manuell oder automatisch an Systemen angebracht werden. Sortieren Sie Systeme nach ihrer Kennzeichnung in Pilotgruppen, und nutzen Sie die Kennzeichnungen als Berichtskriterien.

Die Namenskonvention ist wichtig. Im Idealfall sollten Sie eine Namenskonvention entwickeln, die für alle Personen leicht zu interpretieren ist. Clients werden in der Systemstruktur, in bestimmten Berichten und in den durch Aktivitäten des Clients erzeugten Ereignisdaten durch Ihren Namen identifiziert.

Überprüfen der Integrität von Pilotsystemen

Nachdem die Clients nun identifiziert sind, müssen Sie sicherstellen, dass keine Systemfehler vorhanden sind, die die Bereitstellung beeinträchtigen können. Überprüfen Sie die relevanten Protokolldateien für den ePO-Server sowie die Systemereignisprotokolle. Suchen Sie nach Fehlern, die auf eine nicht ordnungsgemäße Konfiguration und auf Systemanomalien hinweisen und vor dem Installieren von McAfee Host Intrusion Prevention behoben werden müssen. Es folgen einige wichtige Elemente, nach denen gesucht werden sollte:

- **Patch-Status**: Sind alle Treiber und Anwendungen auf dem aktuellen Stand? Es ist bekannt, dass ältere Medien und Audio-Player, Internet Explorer und Treiber für Netzwerkkarten Inkonsistenzen hervorrufen, die Fehler in der Bereitstellung verursachen. Wenden Sie die aktuellen Patches und Hotfixes an.
- **Inkompatible Software**: Werden andere Angriffserkennungs- oder Firewall-Anwendungen auf dem Host ausgeführt? Sie müssen diese deaktivieren oder entfernen.
- **Administratorzugriff**: Sie müssen über Administratorzugriff für das System verfügen. Beachten Sie, ob der Benutzer auch über Administratorzugriff verfügt. Warum? Benutzer stören möglicherweise den Testprozess, wenn sie während des Tests eine neue Anwendung installieren. Platzieren Sie dieses System in einem anderen Verwendungsprofil als Hauptbenutzer, wenn Sie den Benutzeradministratorzugriff nicht entfernen können.
- **Organisatorische Überlegungen**: Einige Systeme erfordern auf Grund der Verwendung einer anderen Sprache, standortspezifischer Anwendungen oder interner Anwendungen besondere Aufmerksamkeit. Berücksichtigen Sie diese Systeme erst in einer zweiten Phase der Bereitstellung, oder schließen Sie spezielle Anwendungen vom IPS-Schutz aus, bis Sie Zeit haben, ihr Verhalten zu protokollieren und zu analysieren.

3. Installieren und Konfigurieren

Installieren Sie auf dem ePO-Server die Host IPS-Erweiterung, die die Schnittstelle für die Host IPS-Richtlinienverwaltung bereitstellt. Importieren Sie den Host IPS-Client in das ePO-Repository.

Suchen Sie im McAfee-Serviceportal (https://mysupport.mcafee.com/Eservice/Default.aspx) nach Patches oder KnowledgeBase-Artikeln. Laden Sie aktualisierten Inhalt von http://www.mcafee.com/us/downloads/ herunter.

Festlegen anfänglicher Schutzstufen und -antworten

Definieren Sie Schutzstufen für jedes Verwendungsprofil, oder weisen Sie sie zu. Wenn Sie die Strategie "das Einfachste zuerst" verfolgen, aktivieren Sie den Basisschutz für ihre standardmäßigen Desktop-Verwendungsprofile. Einzelheiten finden Sie im Produkthandbuch unter *Konfigurieren von IPS-Richtlinien* oder *Konfigurieren von Firewall-Richtlinien*.

Feinabstimmung von Basisrichtlinien (optional)

Einige Administratoren ändern Schutzstandards sofort, bevor Sie mit dem Bereitstellen beginnen. Sie können Anwendungen mit hohem Risiko (Anwendungen, die Dienste oder offene Netzwerk-Ports starten) und interne Anwendungen automatisch schützen. Intern entwickelte Anwendungen sind zu Beginn der Bereitstellung häufig von IPS ausgeschlossen. Dies gilt insbesondere, wenn sie Netzwerkverbindungen überwachen. Interne Softwareentwickler gehen beim Programmieren erwarteter und sicherer Verhaltensweisen möglicherweise nicht so streng vor wie kommerzielle Entwickler. Beispielsweise löst ein Programm, das Links zu Internet Explorer enthält, unbeabsichtigt eine Internet Explorer-Schutzsignatur aus, wenn sich das Programm anders als erwartet verhält. Da intern entwickelte Anwendungen keine typischen Angriffsziele darstellen, stellen sie ein geringeres Sicherheitsrisiko dar.

Fügen Sie die IP-Adressen Ihrer Schwachstellen-Scanner der Liste vertrauenswürdiger Netzwerke hinzu. Ihre vorhandenen ePolicy Orchestrator- und Sicherheitsrichtlinien stellen möglicherweise weitere Informationen zu offensichtlichen Aktivitäten bereit, die für die einzelnen Verwendungsprofile zugelassen oder blockiert werden. Schließlich können Sie den adaptiven Modus verwenden, um Regeln für ausgeschlossene Anwendungen zu definieren und den Schutz zu implementieren. Sie können diesen Schritt ausführen, wenn Sie den Basisschutz eingerichtet und sich mit den IPS-Signaturen und -Richtlinien vertraut gemacht haben.

Benachrichtigen der Benutzer und Planen der Außerkraftsetzung

Benachrichtigen Sie vor der Aktivierung des IPS-Schutzes die Benutzer darüber, dass sie einen neuen Schutz erhalten und sie das System in bestimmten Fällen außer Kraft setzen können. Mit dieser Mitteilung wird das angenommene Risiko für die Benutzerproduktivität reduziert, die insbesondere für Benutzer wichtig ist, die mit Laptops von unterwegs aus zugreifen. Damit die IPS-Blockierung vom Benutzer außer Kraft gesetzt werden kann, muss der Administrator den Benutzern Folgendes bereitstellen:

- Ein Kennwort für einen begrenzten Zeitraum
- Anweisungen zum Deaktivieren von Funktionen
- Möglichkeit zum Entfernen von Host IPS, falls erforderlich

Sie sollten diese Problemumgehungen nicht zu großzügig aushändigen: Schließlich möchten Sie nicht, dass Benutzer das Rollout untergraben. Zwei dieser Problemumgehungen werden später im Pilot entfernt. Einzelheiten finden Sie im Produkthandbuch unter *Definieren der Client-Funktionalität*.

Kontaktieren des Helpdesk-Teams

Lassen Sie den Helpdesk wissen, dass Sie dabei sind, Host IPS zu aktivieren. Obwohl es nur wenige Probleme geben dürfte, sollte der Helpdesk vorbereitet sein, um Symptome zu erkennen, die bei einer Aktivierung des IPS-Schutzes auftreten können.

Installieren von Host IPS auf Pilot-Hosts

Fangen Sie klein an, und installieren Sie nur ein paar Clients. Erweitern Sie den Vorgang dann auf mehr Systeme in größeren Inkrementen, sowie das Vertrauen wächst. Beginnen Sie mit einem, dann mit 10, dann mit 20, dann mit 50 bis zu 100 Systemen. Nachfolgend finden Sie die Rollout-Reihenfolge:

1. Stellen Sie sicher, dass die Zielhosts eingeschaltet sowie mit dem Netzwerk verbunden sind und mit ePolicy Orchestrator kommunizieren.
2. Verwenden Sie einen ePO-Bereitstellungs-Task, um Host IPS-Agenten mithilfe eines Pushs auf eine kleine Gruppe von Hosts in der Pilotgruppe zu übertragen.
3. Validieren Sie die erfolgreiche Installation. Nehmen Sie bei Bedarf Fehlerbehebungen und Anpassungen vor.
4. Erweitern Sie den Schutz auf weitere Systeme.

Überprüfen Sie während der Installation, ob die neue Software auf den Pilotsystemen ordnungsgemäß ausgeführt wird, und überwachen Sie die ePO-Protokolle hinsichtlich Serverereignissen und wesentlicher Auswirkungen auf die Netzwerkleistung. Es können ein paar Probleme auftreten. Aus diesem Grund sind ein Pilot und ein langsames Rollout wichtig. Gehen Sie folgendermaßen vor:

1. Überprüfen Sie, ob die Host IPS-Dienste (FireSvc.exe, mfefire.exe, mfevtp.exe) und der Framework-Dienst (McAfeeFramework.exe) gestartet wurden.
2. Sehr wichtig! Führen Sie einfache Anwendungen wie Buchhaltungs-, Dokumentbearbeitungs-, E-Mail-, Internetzugriffs-, Multimedia- oder Entwicklungs-Tools aus, um zu testen, ob sie ordnungsgemäß ausgeführt werden. Können Ihre Benutzer ihre Standardaufgaben ausführen? Sie sollten die ordnungsgemäße Erkennung während des Betriebs veranschaulichen und validieren.
3. Wenn Sie Probleme auf dem Client feststellen, können Sie die IPS-Client-Protokolle und die Client-Betriebssystemprotokolle auf Fehler überprüfen. Informationen finden Sie im Produkthandbuch unter *Arbeiten mit Host Intrusion Prevention-Clients*.
4. Wiederholen Sie diese Schritte, um den Schutz auf weitere Systeme zu erweitern, bis Sie die Pilotgruppe aufgefüllt haben.

TIPP: Nehmen Sie bei jeder Installation oder Richtlinienänderung Tests vor, um sicherzustellen, dass die Endbenutzer ihre Aufgaben erfolgreich ausführen können. Diese Tests sind möglicherweise die wichtigste Aktivität beim Sicherstellen eines erfolgreichen Rollouts.

4. Grundanpassung

Wenn die Pilotgruppe steht, ist es jetzt Ihre Aufgabe, zu warten und die Situation zu beobachten. Warten Sie zwischen zwei und sieben Tagen, bis eine größere Anzahl an Ereignissen vorliegt, und reagieren Sie auf mögliche Support-Anrufe.

Tägliche Überwachung

Reservieren Sie täglich einige Minuten für die Durchsicht der IPS-Ereignisprotokolle und die Überwachung von Aktivitätsumfang und Aktivitätstypen. Über diese Gewohnheit verschaffen Sie sich Basiswissen zu dem normalen Betrieb und üblichen Aktivitätsmustern. Bei der täglichen Überwachung sollten Sie beispielsweise auf reguläre Vorgänge und Aktivitätsniveaus für Server-Wartung und die Aktualisierung von Anwendungen achten. Ausgehend von diesem Wissen können Sie ungewöhnliche Aktivitäten unmittelbar zum Zeitpunkt ihres Auftretens erkennen.

Die tägliche Durchsicht erleichtert es Ihnen, Regeln, Richtlinien und Ausnahmen im Zusammenhang mit neu auftretenden Ereignissen zu optimieren. Host IPS erlaubt eine fein abgestimmte Kontrolle, da alle System- und API-Aufrufe überwacht und diejenigen blockiert werden, die Schäden anrichten könnten. Ähnlich wie bei Netzwerk-IPS müssen Regeln von Zeit zu Zeit in dem Maß weiter angepasst werden, in dem sich Anwendungen, der geschäftliche Bedarf und Richtlinienanforderungen ändern.

Zu den Aufgaben der fortlaufenden Wartung für eine Host IPS-Ausbringung zählen die Überwachung und Analyse von Vorgängen und ein entsprechendes Reaktionsverhalten, das Ändern und Aktualisieren von Richtlinien sowie das Ausführen von Aufgaben im System, darunter das Einrichten von Benutzerberechtigungen, Server-Tasks, Benachrichtigungen und die Aktualisierung von Inhalten. Diese Aktivitäten müssen unter Wahrung des Betriebs geplant werden, damit Zustand und Wirksamkeit der IPS-Funktionen aufrechterhalten werden.

Überprüfung von Protokollen

Anhand von Ereignisprotokolldaten können Sie Richtlinien optimieren, um ein ausgeglichenes Verhältnis zwischen Schutz und freiem Zugriff auf Informationen und Anwendungen herzustellen. Dieses Gleichgewicht unterscheidet sich im Allgemeinen je nach Benutzertyp. In dieser Phase sollten Sie Richtlinien manuell über den ePO-Server anpassen. Informationen zur automatischen Anpassung von Richtlinien finden Sie unter 5. Aktivieren des adaptiven Modus (optional).

Auf Informationen zu Ereignissen können Sie auf dem ePO-Server unter **Berichterstellung** über die Registerkarte **Host IPS 8.0 | Ereignisse** zugreifen. Sie können die Details für einzelne Ereignisse aufgliedern und beispielsweise ermitteln, durch welchen Vorgang ein Ereignis ausgelöst wurde, zu welchem Zeitpunkt ein Ereignis aufgetreten ist und auf welchem Client. Achten Sie auf rote Markierungen wie False-Positives und Signaturen, für die ein Ereignis mit hohem Schweregrad ausgelöst wurde.

Überprüfen Sie, ob Vorgänge und Dienste einwandfrei sind. Anwendungen, für die Sie dies erwarten, sollten laufen; Anwendungen, für die Sie dies nicht erwarten, sollten nicht angezeigt werden. Wenn Ereignisse zu zulässigen Aktivitäten protokolliert wurden (meist für intern entwickelte Anwendungen), können Sie diese Fälle von False-Positives im nächsten Schritt behandeln.

TIPP: Bei der Durchsicht von Protokolldaten übersehen Sie besondere Situationen, die eine andere Entscheidung zu der entsprechenden Regel nach sich ziehen würden. Machen Sie bei ausführlichen Überprüfungen Pausen, um derartige Fehler zu vermeiden.

Grundanpassung des Schutzes

Setzen Sie sich ausgehend von den Ereignisprotokolldaten die folgenden Ziele:

- Heben Sie den Schutz für protokollierte Ereignisse an, die blockiert werden sollten.
- Eliminieren Sie False-Positives ausgehend von zulässigen geschäftlichen Aktivitäten.

Beginnen Sie mit den folgenden Aktionen:

1 **Reaktionen auf Signaturen bearbeiten**. Berücksichtigen Sie dabei, dass ein Client auf eine der drei folgenden Arten reagieren und entsprechend konfiguriert werden kann:

   - **Ignorieren** – Keine Reaktion. Das Ereignis wird nicht protokolliert und der Vorgang nicht verhindert.
   - **Protokollieren** – Das Ereignis wird protokolliert, der Vorgang jedoch nicht verhindert.
   - **Verhindern** – Das Ereignis wird protokolliert und der Vorgang wird verhindert.

   Wenden Sie die Reaktion "Verhindern" auf alle Signaturen mit hohem Schweregrad an.

2 **Ausnahmen erstellen**. Bestimmen Sie Ereignisse, die legitimes Verhalten melden, das zugelassen oder ggf. zugelassen und protokolliert werden sollte.

Ausnahmeregeln setzen Sicherheitsrichtlinien unter bestimmten Umständen außer Kraft. Sie können Reaktionen so festlegen, dass Ereignisse ignoriert und damit nicht länger protokolliert werden. Beispielsweise ist es möglich, dass bestimmte Skriptverarbeitungsvorgänge gemäß einer Richtlinie als unzulässig gelten, bestimmte Systeme Ihrer Entwicklungsabteilungen jedoch Skripts ausführen müssen. Erstellen Sie Ausnahmen für solche Systeme, damit deren Betrieb normal verläuft, während Skripts auf anderen Systemen weiterhin durch die Richtlinie verhindert werden. Nehmen Sie diese Ausnahmen in einer Serverrichtlinie auf, die nur für die Entwicklungsabteilung gilt.

Mit Ausnahmen verringern Sie die Anzahl von False-Positive-Warnungen und reduzieren die Menge überflüssiger und irrelevanter Daten, die an die Konsole übertragen werden. Durch die Minimierung von Störddaten können Sie wichtige Ereignisse bei der täglichen Überwachung einfacher erfassen.

TIPP: Achten Sie darauf, dass die Ausnahme gerade so allgemein ist, dass diese auf allen ähnlichen Systemen unter denselben oder ähnlichen Bedingungen greift.

3 **Vertrauenswürdige Anwendungen erstellen.**

Vertrauenswürdige Anwendungen sind Anwendungsprozesse, die von allen IPS- und Firewall-Regeln ausgenommen sind. Begrenzen Sie vertrauenswürdige Anwendungen auf Vorgänge, die eine so große Anzahl an False-Positives verursachen, dass genau abgestimmte Ausnahmen einen zu hohen Aufwand nach sich ziehen. Vertrauenswürdige Anwendungen können je nach Benutzerprofil andere sein. Beispielsweise können Sie bestimmte Softwareanwendungen für den technischen Support zulassen, während Sie die Verwendung dieser Programme für die Finanzabteilung verhindern. Sie können diese Anwendungen also auf den Systemen des technischen Supports als vertrauenswürdig festlegen, um ihre Verwendung zuzulassen. Weitere Informationen finden Sie im Produkthandbuch unter *Konfigurieren der Richtlinie "Vertrauenswürdige Anwendungen"*.

4 **Ausführen von Abfragen.**

Mithilfe von Abfragen können Sie Daten zu einzelnen Elementen abfragen und diese Daten nach bestimmten Untermengen filtern, beispielsweise nach Ereignissen hoher Ebene, die von bestimmten Clients für eine bestimmte Zeitspanne gemeldet wurden. Achten Sie auf Signaturen, die besonders häufig Ereignisse auslösen. Handelt es sich dabei um legitime tägliche Geschäftsfunktionen, die zugelassen werden sollten? Legen Sie für diese Signaturen einen geringeren Schweregrad fest. Manche Ausnahmen für Desktop-Computer erweisen sich als Fehlverhalten zulässiger Anwendungen, das Sie nicht zulassen müssen. Vergewissern Sie sich, dass die Benutzeranwendung einwandfrei funktioniert, und lassen Sie das Fehlverhalten weiterhin blockieren.

TIPP: Es kommt häufig vor, dass Ereignisse generiert und blockiert werden, ohne dass dies spürbare Auswirkungen für Benutzer oder den Betrieb einer Anwendung hat. VMware-Umhüllungen und Adobe-Anwendungen weisen oft ein solches Verhalten auf. Diese Ereignisse können bedenkenlos ignoriert werden, sofern Sie bestätigen können, dass die Benutzerfreundlichkeit unverändert ist. Möglicherweise schließen Sie eine Sicherheitslücke wie eine Schwachstelle im Site-übergreifenden Skripting, die sonst ausgenutzt werden kann.

Anpassungsprozess

Haben Sie Beschwerden von Benutzern erhalten? Setzen Sie sich direkt mit diesen in Verbindung und prüfen Sie, ob Anwendungen richtig funktionieren. Halten Sie sich für die Entscheidungen zur Anpassung in der Testphase an den folgenden Ablauf:

1. **Richtlinien bearbeiten** – Erstellen und bearbeiten Sie Richtlinien und Reaktionen mit ePolicy Orchestrator.
2. **Richtlinien gezielt anwenden** – Wenden Sie die Richtlinien mit ePolicy Orchestrator auf die Zielsysteme an.
3. **Änderungen aktivieren** – Wenn Sie Host IPS-Richtlinien über die ePO-Konsole ändern, werden die Änderungen bei der nächsten Kommunikation zwischen Agent und Server für die verwalteten Systeme übernommen. Standardmäßig ist dieses Zeitintervall auf 60 Minuten festgelegt. Um Richtlinien mit sofortiger Wirkung anzuwenden, können Sie von der ePO-Konsole aus eine Agenten-Reaktivierung durchführen.
4. **Änderungen testen** – Überprüfen Sie für diese Änderungen erneut den einwandfreien Betrieb einschließlich der Kompatibilität mit Unternehmenssystemen (unter Zulassung legitimer Aktivität). Sorgen Sie dafür, dass der IPS-Netzwerkverkehr möglichst gering ist und Sie die Zahl der erfassten False-Positives senken.
5. **Richtlinien in der Breite anwenden** – Wenn die neuen Richtlinien funktionieren, können Sie diese für die relevanten Systeme übernehmen.
6. **Tägliche Überwachung fortsetzen**.

Einzelheiten zur Verwendung von IPS-Richtlinien finden Sie im Produkthandbuch unter *Konfigurieren von IPS-Richtlinien*. Dieser Abschnitt enthält auch Informationen zum Einrichten von Signaturreaktionen und dem Erstellen von Ausnahmen und vertrauenswürdigen Anwendungen auf Grundlage von Ereignissen. Details zur Verwendung von Firewall-Richtlinien finden Sie im Produkthandbuch unter *Konfigurieren von Firewall-Richtlinien*.

Konfigurieren von Dashboards und Berichten

Die Ereignisse sind jetzt geordneter und genauer erfasst, sodass Sie die Strukturierung und Kommunikation von IPS- und Firewall-Informationen mithilfe des ePO-Servers optimieren können.

- Konfigurieren Sie ePO-Dashboards, um einen schnellen Überblick über die jeweilige Richtlinien-Compliance, Ereignistrends, Abfrageergebnisse und bestehende Probleme zu erhalten. Speichern Sie bestimmte Dashboards, um die tägliche Überwachung, die wöchentliche Überprüfung und Verwaltungsberichte festzuhalten.
- Konfigurieren Sie Benachrichtigungen, damit bei bestimmten Ereignissen die zuständigen Mitarbeiter gewarnt werden. Beispielsweise ist eine Konfiguration möglich, bei der eine Benachrichtigung gesendet wird, wenn auf einem bestimmten Server ein Ereignis hohen Schweregrads ausgelöst wurde.
- Sie können Berichte für die automatische Ausführung und Versendung als E-Mail an zuständige Personen planen.

Einzelheiten zur Verwendung von Dashboards und Berichten finden Sie im Produkthandbuch unter *Verwaltung Ihres Schutzes*.

Wartezeit und Beobachtung

Überwachen Sie Ereignisse für mindestens weitere zwei Wochen täglich, und achten Sie dabei insbesondere auf Helpdesk-Anrufe, Anomalien und False-Positives. Bei dieser eher konservativen Rollout-Strategie sollte es nur zu wenigen Support-Anrufen und Problemen kommen und daher eine nur geringe Zahl an Anpassungen erforderlich sein.

Stellen Sie außerdem sicher, dass Workarounds außer Kraft gesetzt sind und so verhindert wird, dass Benutzer oder Malware den IPS-Schutz umgehen. Lassen Sie keinesfalls die Deaktivierung von Modulen oder das Entfernen des Host IPS-Clients zu.

5. Aktivieren des adaptiven Modus (optional)

Beginnen Sie nach dem Abschluss eines Geschäftszyklus mit der eingerichteten Software mit dem Implementieren gezielter Regeln, um benutzerdefinierte Richtliniengruppen zu erstellen. Diese Richtlinien können manuell definiert werden. Der adaptive Modus bietet jedoch ein leistungsstarkes Tool zum Erstellen von IPS-Regelrichtlinien basierend auf der Hostaktivität und ohne Interaktion des Administrators. Da eine Anwendung verwendet wird, wird eine Ausnahme erstellt, um alle Aktionen zuzulassen. Im adaptiven Modus werden keine IPS-Ereignisse ausgelöst, und es wird keine Aktivität blockiert. Dies gilt nicht für bösartige Angriffe (Signaturen mit hohem Schweregrad). Ausnahmen werden vom ePO-Server als IPS-Client-Regeln protokolliert, damit Sie den Fortschritt überwachen können.

Indem Sie für repräsentative Hosts während der Pilotphase den adaptiven Modus festlegen, können Sie für jedes Verwendungsprofil oder jede Anwendung eine Abstimmungskonfiguration erstellen. Die IPS-Funktion ermöglicht es Ihnen anschließend, beliebige, alle oder keine Client-Regeln anzuwenden und sie in Serverrichtlinien umzuwandeln. Deaktivieren Sie den adaptiven Modus, wenn die Abstimmung abgeschlossen ist, um den Eindringschutz des Systems zu erhöhen.

Mit dem Protokollierungsmodus konnten Sie die Häufigkeit von Aktivitäten nachvollziehen. Entsprechend erfahren Sie im adaptiven Modus das volle Ausmaß und den Typ von Aktivitäten. Diese beiden Tools zusammen bieten eine gute Funktionsbasis für die legitimen Geschäftsaktivitäten Ihrer Organisation. Sie sollten mit unregelmäßigen Aktivitäten rechnen, die während der Pilotphase nicht erfasst werden. Stellen Sie sich darauf ein, dass Sie Ausnahmen überprüfen und bei Bedarf Regeln manuell erstellen müssen. Ein Benutzer führt beispielsweise alle vier Monate einmal eine Anwendung aus und verpasst die Protokollierungsphase und die Phase des adaptiven Modus.

Im adaptiven Modus werden alle Signaturen mit hohem Schweregrad standardmäßig blockiert. Verwenden Sie daher den adaptiven Modus, um Signaturen mit mittlerem und hohem Schweregrad zu verwalten. Diese Kombination bietet Ihnen einen guten Überblick über die Aktivitäten ohne viele Stördaten.

Im adaptiven Modus werden Ausnahmeregeln sehr effizient erstellt. Es ist jedoch unwahrscheinlich, dass alle Aktivitäten auf einem bestimmten System zugelassen sind oder Sie keine neuen Schutzmaßnahmen in Betracht ziehen. Aus diesem Grund sollten Sie den adaptiven Modus nur für einen begrenzten Zeitraum verwenden. Überprüfen Sie alle erstellten Ausnahmen (es gibt nur eine Instanz für jede Ausnahme), und deaktivieren Sie unzulässige Regeln, die im adaptiven Modus erstellt werden.

Wenn Sie den adaptiven Modus anwenden, wählen Sie die Richtlinienoption **Client-Regeln speichern** aus. Andernfalls werden die neuen Regeln in jedem Richtlinienerzwingungsintervall gelöscht und müssen neu erstellt werden. Wenn Sie letztlich den adaptiven Modus deaktivieren und zur Erzwingung wechseln, deaktivieren Sie die Option **Client-Regeln speichern**, und entfernen Sie alle Regeln, die nicht von einer durch ePO bereitgestellten Richtlinie erzwungen werden.

Anwenden des adaptiven Modus

1. Wenden Sie den adaptiven Modus für einen bestimmten Zeitraum an (eine bis vier Wochen).
2. Bewerten Sie die Client-Regeln.
3. Deaktivieren Sie unangemessene Regeln.
4. Verschieben Sie legitime Client-Regeln auf der Registerkarte **IPS-Client-Regeln** direkt in eine Richtlinie für Anwendungen auf anderen Clients.
5. Deaktivieren Sie den adaptiven Modus.

6 Heben Sie die Auswahl der Option **Client-Regeln speichern** auf, wenn sie ausgewählt ist.

TIPP: Denken Sie daran, den adaptiven Modus zu deaktivieren, damit keine Regeln ohne Ihr Wissen erstellt werden.

Empfohlene Vorgehensweisen

- Führen Sie Clients mindestens eine Woche im adaptiven Modus aus, um alle normalen Aktivitäten zu ermitteln. Wählen Sie Zeiträume aus, in denen geplante Aktivitäten wie Sicherungen oder Skripterstellungen ausgeführt werden.
- Verfolgen Sie Client-Regeln in der ePO-Konsole nach, und prüfen Sie sie in der normalen, gefilterten und aggregierten Ansicht.
- Verwenden Sie automatisch erstellte Client-Regeln, um neue ausführlichere Richtlinien zu erstellen, oder fügen Sie vorhandenen Richtlinien neue Regeln hinzu, und wenden Sie die aktualisierten Richtlinien dann auf andere Clients an.
- Wählen Sie die Richtlinienoption **Client-Regeln speichern** aus. Wenn Sie sie nicht auswählen, werden die Regeln nach jedem Richtlinienerzwingungsintervall gelöscht.
- Überprüfen Sie die erstellten Ausnahmen. Deaktivieren Sie den adaptiven Modus, wenn Sie die Überprüfung nicht vornehmen können, um zu vermeiden, dass risikoreiche Aktivitäten zugelassen werden.
- Aktivieren Sie den adaptiven Modus kurz, um Ausnahmen für eine neue Anwendung zu erstellen, und fügen Sie sie dann einer Richtlinie hinzu.

Einzelheiten zum Verwenden von IPS-Richtlinien im adaptiven Modus finden Sie im Produkthandbuch unter *Konfigurieren von IPS-Richtlinien*. Einzelheiten zum Verwenden von Firewall-Richtlinien im adaptiven Modus finden Sie im Produkthandbuch unter *Konfigurieren von Firewall-Richtlinien*.

HINWEIS: Im adaptiven Modus können adaptive und nicht adaptive Aktivitäten ausgeführt werden. Regeln, von denen diese Aktivitäten zugelassen werden, werden ohne Bestätigung des Administrators erstellt. Pro erstellter Regel wird nur ein Ausnahmeereignis protokolliert. Daher werden dieselben Aktivitäten nach dem Erstellen der Regel nicht dokumentiert. Sie erhalten nur eine Benachrichtigung. Aus diesem Grund müssen Sie sorgfältig prüfen und antworten, um unzulässige Regeln zu verhindern.

6. Feinabstimmung

Nachdem Sie die Basisantworten für Aktivitäten erstellt und abgestimmt haben, können Sie mit dem Erhöhen der Schutz- und Erzwingungsstufen beginnen. Wählen Sie dazu die entsprechende Kategorie der Richtlinie **IPS-Schutz** aus. Diese Abstimmungsschritte können im Rahmen einer täglichen Überwachung ausgeführt werden. Möglicherweise möchten Sie aber eher die formalen iterativen Schritte des Pilots wiederholen. Warten Sie nach jedem Schritt mindestens zwei Wochen, bevor Sie weitere Änderungen in Betracht ziehen, um sicherzustellen, dass die Systeme unter den vorhandenen Schutzstufen ordnungsgemäß ausgeführt werden.

Basisschutz, erweiterter und maximaler Schutz

Mit der Kategorie **Erweiterter Schutz** der Richtlinie "IPS-Schutz" werden Signaturen mit hoher und mittlerer Sicherheitsstufe verhindert, und der Rest wird ignoriert. Mit der Kategorie **Erweiterten Schutz vorbereiten** der Richtlinie wird zunächst der Zwischenschritt ausgeführt, bei dem die mittleren Sicherheitsstufen protokolliert werden. Die Protokollierung bietet

ausführliche Informationen darüber, welche Aktivitäten betroffen sind, wenn Sie die Schutzstufe erhöhen. Sie dient als Hilfe bei der Richtlinienverwaltung und kann die Anzahl böser Überraschungen reduzieren.

Wenn die Geschäftsabläufe ohne Störungen fortgesetzt werden, können Sie statt der Basiseinstellungen den erweiterten Schutz verwenden. Wiederholen Sie diese Aktionen für die anderen Systeme in Ihrem Netzwerk. Die Kategorie **Maximaler Schutz** der Richtlinie eignet sich für die dediziertesten und gesichertsten Betriebsumgebungen. Da beim maximalen Schutz auch Signaturen mit geringem Schweregrad blockiert werden, sollte dieser Schutz sehr umsichtig und nach einer umfassenden Testphase bereitgestellt werden. Verwenden Sie die Kategorie **Maximalen Schutz vorbereiten** zu Testzwecken, um die Auswirkungen von Änderungen zu ermitteln, bevor Sie den maximalen Schutz aktivieren.

Extrem konservative Organisationen können für jede Änderung in der Schutzstufe ein Rollout als eigenen Pilot vornehmen, auf die dann die erläuterten iterativen Schritte folgen. Denken Sie daran, Notsysteme und den adaptiven Modus vor und nach den Testzyklen, in denen Änderungen validiert werden, zu aktivieren und zu deaktivieren.

Fortsetzen der Abstimmung

Überprüfen Sie auftretende Ausnahmen und Fehler. Bearbeiten Sie sie wie im anfänglichen Abstimmungsschritt erläutert.

- Überprüfen Sie Helpdesk-Anrufe und Benutzerkommentare hinsichtlich Beschwerden oder Geschäftsproblemen, die durch blockierten Zugriff auftreten, falscher Positiva oder neuer Anwendungsverhalten. Diese Probleme dürften nur in sehr geringer Anzahl auftreten, es gibt jedoch immer neue Anforderungen.
- Überprüfen Sie regelmäßig die generierten Ausnahmen.
- Stimmen Sie Richtlinien entsprechend ab. Verwenden Sie den ePO-Server, um Richtlinienaktualisierungen an Hostsysteme zu senden. Sie müssen sie bewusst auf die Systeme anwenden, die Sie einschließen möchten.

7. Ausführen der Wartung und Erweiterung

Die vorherigen Schritte erläutern den grundlegenden Rollout-Prozess. Sobald auf Ihren Systemen die mittleren Schutzstufen bereitgestellt sind, besteht erweiterter Systemschutz. Sie müssen regelmäßig Überwachungen vornehmen, Richtlinien aktualisieren und Systeme verwalten. Ziehen Sie nun auch die Erweiterung der zu schützenden Systeme und die Verbesserung des Schutzes in Erwägung, und schließen Sie strengere Richtlinien und andere Host IPS-Funktionen ein.

Verwaltung

McAfee veröffentlicht häufig Inhaltsaktualisierungen für neue Signaturen und vereinzelt auch Funktionsaktualisierungen und Patches. Vorschläge für bewährte Methoden umfassen Folgendes:

- Legen Sie einen regelmäßigen Aktualisierungszeitplan fest, damit der ePO-Server Aktualisierungen aus dem McAfee-Repository abruft und Ihre Clients diese Aktualisierungen erhalten.
- Rufen Sie Host IPS-Inhalt für den Testzweig Ihres Repository zum Testen einer Pilotsystemgruppe auf, wenn Sie über eine große Anzahl von benutzerdefinierten Anwendungen verfügen, für die während der ersten Rollouts eine Abstimmung erforderlich war. Sobald der neue Inhalt von der Pilotgruppe zertifiziert wurde, können Sie ihn in den aktuellen Zweig für die gesamte Bereitstellung verschieben.

- Planen Sie Inhaltsdownloads so, dass sie mit den Veröffentlichungen vom "Patch-Dienstag" zusammen erfolgen, wenn Sie Microsoft-Produkte verwenden.
- Verwenden Sie den adaptiven Modus, um Profile für bestimmte Systeme zu erstellen, und leiten Sie die resultierenden Client-Regeln an den Server weiter, wenn neue Anwendungen installiert werden. Möglicherweise verfügen Sie über die Zeit und Ressourcen, um sie unmittelbar abzustimmen. Sie können diese Client-Regeln auf vorhandene oder neue Richtlinien übertragen und dann die Richtlinie auf andere Computer anwenden, um die neue Software zu verwalten.
- Übernehmen Sie die IPS-Tests in Ihre Änderungsmanagement- und Software-veröffentlichungsprozesse. Wenn Sie die Bereitstellung eines Patches, Service Packs oder Produkts von Microsoft vorbereiten, sollten Sie sie auf IPS-Systemen testen und kontrollieren, damit die ordnungsgemäße Abstimmung vor der allgemeinen Veröffentlichung vorgenommen werden kann.

Erweiterung

Verwenden Sie in Abhängigkeit Ihrer Organisation eine der folgenden Optionen zum Erweitern der Bereitstellung. Gehen Sie bei der Ausbringung von Änderungen langsam und bewusst vor, damit Sie Ausfälle bei Benutzern minimieren und Anomalien schnell diagnostizieren können. Es ist besser, langsam vorzugehen, als Fehler zu machen oder hilfreiche Schutzoptionen auszulassen.

Gehen Sie für die Erweiterung folgendermaßen vor:

- Stellen Sie denselben Schutz auf allen zusätzlichen Systemen mit den getesteten Verwendungsprofilen bereit. Sie können die Bereitstellung von Host IPS auf Tausenden von Computern auf einfache Weise verwalten, da die meisten Computer ein paar Verwendungsprofilen zugeordnet werden können. Die Verwaltung einer großen Bereitstellung reduziert sich auf die Verwaltung einiger weniger Richtlinienregeln.
- Wiederholen Sie diesen Prozess für Hauptbenutzer und Server, wenn Sie nur standardisierte Desktops in den Pilot aufgenommen haben. Beginnen Sie mit der Protokollierung, und nutzen Sie die Vorteile des adaptiven Modus.
- Fügen Sie neue Verwendungsprofile und Benutzer-Communitys hinzu.
- Implementieren Sie Firewall-Regeln. Befolgen Sie den Pilotprozess, aber lesen Sie Einzelheiten zu Regeln und dem Lernmodus im Produkthandbuch nach.

Installieren von ePolicy Orchestrator

Für diese Version von Host Intrusion Prevention (HIP) müssen Sie abhängig vom erworbenen Schutzumfang und der ausgeführten Version von ePolicy Orchestrator mindestens eine Erweiterung installieren.

Nachfolgende finden Sie die Liste der erforderlichen Erweiterungen:

Tabelle 3: Nur Firewall-Funktion

McAfee ePO-Version	Dateiname	Erforderliche Erweiterungen	Funktionalität
4.0	**HOSTIPS_8000.zip**	Host Intrusion Prevention 8.0.0	Firewall-Funktion
	help_epo_103x.zip	ePO-Hilfe	ePO-Hilfe mit Host Intrusion Prevention 8.0-Informationen
4.5	**HOSTFW_8000_45.zip**	Host Intrusion Prevention 8.0.0	Firewall-Funktion
		Host IPS Advanced-Erweiterung	Automatisches Antworten*
		Hilfeinhalt: hip_800_help	ePO-Hilfe mit Host Intrusion Prevention 8.0-Informationen
4.6	**HOSTFW_8000_46.zip**	Host Intrusion Prevention 8.0.0	Firewall-Funktion
		Host IPS Advanced-Erweiterung	Automatisches Antworten*
		Inhalt der Hilfe: hip_800_help	ePO-Hilfe mit Host Intrusion Prevention 8.0-Informationen

* Nur gültig, wenn die Host Intrusion Prevention 8.0.0-Erweiterung installiert ist.

Tabelle 4: IPS- und Firewall-Funktionen

McAfee ePO-Version	Dateiname	Erforderliche Erweiterungen	Funktionalität
4.0	**HOSTIPS_8000.zip**	Host Intrusion Prevention 8.0.0	Firewall-Funktion
	HostIPSLicense.zip	Host IPS-Lizenzerweiterung	IPS-Funktion*
	help_epo_103x.zip	ePO-Hilfe	ePO-Hilfe mit Host Intrusion Prevention 8.0-Informationen
4.5	**HOSTIPS_8000_45.zip**	Host Intrusion Prevention 8.0.0	Firewall-Funktion
		Host IPS Advanced-Erweiterung	Automatisches Antworten*
		Host IPS-Lizenzerweiterung	IPS-Funktion*
		Inhalt der Hilfe: hip_800_help	ePO-Hilfe mit Host Intrusion Prevention 8.0-Informationen
4.6	**HOSTIPS_8000_46.zip**	Host Intrusion Prevention 8.0.0	Firewall-Funktion
		Host IPS Advanced-Erweiterung	Automatisches Antworten*
		Host IPS-Lizenzerweiterung	IPS-Funktion*

McAfee ePO-Version	Dateiname	Erforderliche Erweiterungen	Funktionalität
		Inhalt der Hilfe: hip_800_help	ePO-Hilfe mit Host Intrusion Prevention 8.0-Informationen

* Nur gültig, wenn die Host Intrusion Prevention 8.0.0-Erweiterung installiert ist.

Die einzelnen Erweiterungen für ePolicy Orchestrator 4.5 und 4.6 enthalten mehrere ZIP-Dateien, die als separate Erweiterungen installiert werden – eine für jeden Funktionalitätstyp wie oben aufgeführt. Wenn Sie Host Intrusion Prevention 8.0 für ePolicy Orchestrator 4.0 installiert haben und eine Aktualisierung auf Version 4.5 oder 4.6 vornehmen, müssen Sie zwei zusätzliche Erweiterungen installieren: die Host IPS Advanced-Erweiterung (HostIpsAdv.zip) und die Hilfeinhaltserweiterung (help_hip_800.zip). Installieren Sie dazu die einzelne Host Intrusion Prevention-Erweiterung für die entsprechende Version von ePolicy Orchestrator, oder öffnen Sie die einzelne Erweiterung, und installieren Sie die fehlenden Erweiterungen. Der Inhalt der einzelnen Erweiterungs-ZIPs lautet folgendermaßen:

Tabelle 5: Inhalt der aus mehreren ZIPs bestehenden Erweiterungen

HOSTFW_8000_45.zip	HOSTFW_8000_46.zip	HOSTIPS_8000_45.zip	HOSTIPS_8000_46.zip
• HOSTIPS_8000.zip • HostIpsAdv.zip • help_hip_800.zip	• HOSTIPS_8000_Lite.zip • HostIpsAdv.zip • help_hip_800.zip	• HOSTIPS_8000.zip • HostIPSLicense.zip • HostIpsAdv.zip.zip • help_hip_800.zip	• HOSTIPS_8000_Lite.zip • HostIPSLicense.zip • HostIpsAdv.zip • help_hip_800.zip

Inhalt

▸ Installieren der Erweiterung
▸ Entfernen der Erweiterung

Installieren der Erweiterung

Fügen Sie die Produkterweiterungsdatei in ePolicy Orchestrator hinzu, um Host Intrusion Prevention zu installieren. Nutzen Sie diesen Prozess zum Aktualisieren oder Ersetzen einer Host-IPS-Erweiterung.

Vorbereitung

Wenn Host Intrusion Prevention 6.1/7.0-Erweiterungen installiert sind, nehmen Sie zunächst eine Aktualisierung auf die Host Intrusion Prevention 7.0.5-Erweiterung vor, und installieren Sie dann die Host Intrusion Prevention 8.0-Erweiterung. Dadurch wird eine erfolgreiche Installation und Migration der Richtlinien für Version 8.0 sichergestellt.

Aufgabe

1. Wechseln Sie zu **Konfiguration | Erweiterungen** (ePolicy Orchestrator 4.0), oder wählen Sie **Software | Erweiterungen** (ePolicy Orchestrator 4.5 und höher) aus.
2. Klicken Sie auf **Erweiterung installieren**.
3. Geben Sie im Dialogfeld **Erweiterung installieren** den Pfad zur erforderlichen Host-IPS-Erweiterungsdatei an, und klicken Sie auf **OK**.

   HINWEIS: Dieser Vorgang kann einige Minuten dauern.

4 Klicken Sie nach der Installation der Erweiterung und der Anzeige des Übersichtsbildschirms auf **OK**.

5 Wiederholen Sie die Schritte 2 bis 4, um bei Bedarf zusätzliche Erweiterungen zu installieren.

- In ePolicy Orchestrator 4.0 werden die Host Intrusion Prevention 8.0.0- und die Host IPS-Lizenzerweiterung in der Liste **Verwaltete Produkte** unter den Erweiterungen angezeigt, sofern sie installiert sind.
- In ePolicy Orchestrator 4.5 und 4.6 wird Host Intrusion Prevention in der Liste **Verwaltete Produkte** unter den Erweiterungen angezeigt, und alle für das Produkt installierten Erweiterungen werden im rechten Bereich angezeigt.

Entfernen der Erweiterung

Wenn Sie Host Intrusion Prevention 8.0 vom ePolicy Orchestrator-Server entfernen möchten, entfernen Sie die entsprechenden Erweiterungen.

HINWEIS: Wenn Sie die Erweiterungen entfernen, entfernen Sie alle Richtlinien und Richtlinienzuweisungen. Diese Aktion wird nur als Teil eines Fehlerbehebungsverfahrens empfohlen, wenn dies in Absprache mit dem McAfee-Support geschieht.

- Für ePolicy Orchestrator 4.0: Wechseln Sie zu **Konfiguration | Erweiterungen**, wählen Sie in der Liste **Verwaltete Produkte** den Eintrag **Host Intrusion Prevention 8.0.0** (oder **Host IPS License Extension**, falls installiert) aus, und klicken Sie dann auf **Entfernen**.
- Für ePolicy Orchestrator 4.5 und höher: Wählen Sie **Software | Erweiterungen** aus, wählen Sie in der Liste **Verwaltete Produkte** den Eintrag **Host Intrusion Prevention** aus, und klicken Sie auf der linken Seite auf den Link **Entfernen** der installierten Erweiterung.

HINWEIS: Wenn mehrere Host Intrusion Prevention 8.0-Erweiterungen installiert sind, müssen Sie sie in dieser Reihenfolge entfernen:

1 Host IPS License Extension

2 Host IPS Advanced Extension

3 Host Intrusion Prevention 8.0.0

Wenn Sie die Host IPS-Lizenzerweiterung entfernen und diese dann erneut installieren, sind sowohl das Eindringungsschutzsystem auf Host-Ebene als auch die Funktion für Netzwerk-IPS deaktiviert und müssen manuell in der Richtlinie für die IPS-Optionen aktiviert werden.

Migrieren von Richtlinien

Sie können die Richtlinien von McAfee Host Intrusion Prevention Version 6.1 oder 7.0 erst für Clients der Version 8.0 verwenden, nachdem Sie die Richtlinien von Version 6.1 oder 7.0 zum Format von Version 8.0 migriert haben. Host Intrusion Prevention 8.0 bietet mithilfe der ePolicy Orchestrator-Funktion **Host IPS-Richtlinienmigration** unter **Automatisierung** eine einfache Möglichkeit zum Migrieren von Richtlinien. Diese Migration umfasst das Übertragen und Verschieben von Richtlinien. Nachdem die Richtlinie migriert wurde, wird sie im Richtlinienkatalog unter der entsprechenden Host IPS 8.0-Produktfunktion und -kategorie angezeigt, wobei **[6.1]** oder **[7.0]** auf den Namen der Richtlinie folgt.

Alle Richtlinien außer den folgenden werden in die entsprechenden Richtlinien von Version 8.0 übertragen und zu diesen migriert:

- Richtlinien für die Anwendungsblockierungsoptionen werden häufig nicht migriert. (Diese Richtlinien wurden in Version 8.0 entfernt.)
- Richtlinien für die Anwendungsblockierungsregeln werden zu IPS-Regelrichtlinien mit dem Namen "Application Hooking and Invocation Protection" <Name> [6.1 oder 7.0] migriert. (Diese Richtlinien wurden in Version 8.0 entfernt.) Nachdem diese Richtlinien zu IPS-Regelrichtlinien migriert wurden, sind ihre Anwendungsschutzregeln leer, und die Ausnahmeliste umfasst alle vertrauenswürdigen Standardanwendungen, die auf "Vertrauenswürdig für Application Hooking" festgelegt sind. Damit Sie diese migrierte Richtlinie verwenden können, müssen Sie in einer Einstellung mit mehreren Richtlinieninstanzen auch die Richtlinie "Meine Standard-IPS-Regeln" zuweisen, da diese durch die Inhaltsaktualisierungen die neueste Anwendungsschutzliste enthält.

  HINWEIS: Anwendungen, bei denen das Einklinken in den Richtlinien für die Anwendungsblockierungsregeln gesperrt ist, werden nicht migriert und müssen den Anwendungsschutzregeln in der IPS-Regelrichtlinie nach der Migration manuell hinzugefügt werden.

- Die Richtlinien für die Firewall-Quarantäne-Optionen werden nicht migriert. (Diese Richtlinien wurden in Version 8.0 entfernt.)
- Die Richtlinien für die Firewall-Quarantäne-Regeln werden nicht migriert. (Diese Richtlinien wurden in Version 8.0 entfernt.)
- IPS-Client-Regeln und Firewall-Client-Regeln werden nicht migriert.

HINWEIS: Richtlinienzuweisungen werden bei der Migration automatisch übernommen, wenn die Vererbung nicht unterbrochen wurde. Überprüfen Sie die Richtlinienzuweisungen immer nach dem Migrieren von Richtlinien.

Migrationszenarien

Die Migration von Richtlinien zu Version 8.0 erfolgt für 6.1- und 7.0-Richtlinien auf ähnliche Weise. Dies gilt für alle Plattformen.

Zum Migrieren von dieser Version von Host Intrusion Prevention...	Zu Version 8.0 gehen Sie folgendermaßen vor...
6.1	• Installieren Sie die Host IPS 8.0-Erweiterungen in ePolicy Orchestrator. • Migrieren Sie die Richtlinien von Version 6.1 zu Richtlinien von Version 8.0, indem die die Migrationsfunktion von Host IPS 8.0 ausführen. Überprüfen Sie die migrierten Richtlinien und Richtlinienzuweisungen. • Stellen Sie Host IPS 8.0-Clients bereit, um die Host IPS 6.1-Clients zu ersetzen. • Stellen Sie das aktuelle Inhaltsupdate für Host IPS 8.0-Clients bereit.
7.0.x	• Installieren Sie die Host IPS 8.0-Erweiterungen in ePolicy Orchestrator. • Migrieren Sie die Richtlinien von Version 7.0 zu Richtlinien von Version 8.0, indem Die die Migrations-Funktion von Host IPS 8.0 ausführen. Überprüfen Sie die migrierten Richtlinien und Richtlinienzuweisungen. • Stellen Sie Host IPS 8.0-Clients bereit, um die Host IPS 7.0-Clients zu ersetzen. • Stellen Sie das aktuelle Inhaltsupdate für Host IPS 8.0-Clients bereit.

TIPP: Wenn Host Intrusion Prevention 6.1/7.0-Erweiterungen installiert sind, nehmen Sie zunächst eine Aktualisierung auf die Host Intrusion Prevention 7.0.5-Erweiterung vor, und installieren Sie dann die Host Intrusion Prevention 8.0-Erweiterung. Dadurch werden eine erfolgreiche Installation der Richtlinien von Version 8.0 und ihre Migration sichergestellt.

Inhalt

▸ Migrieren von Richtlinien aus früheren Versionen
▸ Migrieren von Richtlinien über eine XML-Datei

Migrieren von Richtlinien aus früheren Versionen

Wenn die McAfee Host Intrusion Prevention 6.1- oder 7.0-Erweiterungen auch nach dem Installieren von Host Intrusion Prevention 8.0 noch in ePolicy Orchestrator vorhanden sind, besteht die einfachste Möglichkeit zum Migrieren *aller* vorhandenen Richtlinien darin, die Richtlinien direkt zu migrieren.

Aufgabe

1. Klicken Sie auf **Automatisierung | Host IPS-Richtlinienmigration**.
2. Klicken Sie unter **Aktion** bei den Host IPS 6.1-Richtlinien oder den Host IPS 7.0-Richtlinien im ePO-Richtlinienkatalog auf **Migrieren**.
3. Klicken Sie nach abgeschlossener Richtlinienmigration auf **Schließen**.
   Alle Richtlinien von Version 6.1 oder 7.0 IPS sowie der Firewall-Funktion und der Funktion "Allgemein" werden in Version 8.0 konvertiert, und hinter dem Namen wird [6.1] oder [7.0]

angezeigt. Die Richtlinien für die Anwendungsblockierungsregeln werden in Application Hooking Protection [6.1] oder [7.0] IPS-Regelrichtlinien konvertiert.

HINWEIS: Wenn Sie die Richtlinienmigration ein zweites Mal ausführen, werden alle zuvor migrierten Richtlinien mit demselben Namen überschrieben. Dieser Vorgang ist nicht selektiv, da alle vorhandenen Richtlinien von Version 6.1 oder 7.0 migriert werden. Wenn Sie Richtlinien selektiv migrieren möchten, müssen Sie die Migration über eine XML-Datei vornehmen.

Migrieren von Richtlinien über eine XML-Datei

Wenn die McAfee Host Intrusion Prevention 6.1- oder 7.0-Erweiterung nicht installiert ist und Sie ausgewählte einzelne Richtlinien zuvor in eine XML-Datei exportiert haben oder Richtlinien selektiv migrieren möchten, müssen Sie die Migration über eine XML-Datei vornehmen. Der Vorgang beinhaltet das Exportieren von 6.1- oder 7.0-Richtlinien in das XML-Format, das Konvertieren des Inhalts der XML-Datei in McAfee Host Intrusion Prevention 8.0-Richtlinienversionen und das anschließende Importieren der migrierten XML-Datei in den Host IPS 8.0-Richtlinienkatalog.

Vorbereitung

Dieser Vorgang kann nur verwendet werden, wenn bereits eine XML-Datei mit exportierten Richtlinien vorliegt. Klicken Sie auf der Seite "Richtlinienkatalog" oder auf der Seite der entsprechenden Host IPS-Richtlinie auf **Exportieren**, um die Richtlinien in eine XML-Datei zu exportieren.

Aufgabe

1. Klicken Sie auf **Automatisierung | Host IPS-Richtlinienmigration**.
2. Klicken Sie unter **Aktion** bei den Host IPS 7.0-Richtlinien in einer XML-Datei auf **Migrieren**.
3. Wählen Sie im Dialogfeld mit der Richtlinien-XML-Datei die XML-Datei der Host IPS-Version 6.1 oder Host IPS-Version 7.0 aus, die migriert werden soll, und klicken Sie dann auf **OK**. Die XML-Datei wird in das Richtlinienformat von Version 8.0 konvertiert.
4. Klicken Sie mit der rechten Maustaste auf den Link der konvertierten XML-Datei, und speichern Sie sie für den Import.
5. Importieren Sie die XML-Datei in den ePO-Richtlinienkatalog. Einzelheiten zum Importieren und Exportieren von Richtlinien finden Sie in der Dokumentation zu ePolicy Orchestrator.

Installieren des Windows-Clients

In diesem Abschnitt finden Sie Informationen zu den Anforderungen und Eigenschaften sowie zur Installation des McAfee Host Intrusion Prevention 8.0-Windows-Clients für Workstations und Server.

Inhalt

- Details zum Windows-Client
- Remote-Installation des Windows-Clients
- Lokale Installation des Windows-Clients
- Anwenden von Richtlinien und IPS-Inhaltsaktualisierungen
- Entfernen des Windows-Clients

Details zum Windows-Client

Diese Version des McAfee Host Intrusion Prevention 8.0-Clients für Windows kann mit ePolicy Orchestrator 4.0 und höher, McAfee Agent 4.0 und höher sowie der McAfee Host Intrusion Prevention 8.0-Erweiterung verwendet werden. Detaillierte Informationen zur Installation und Verwendung von ePolicy Orchestrator sowie zu den Anforderungen an das System, die Datenbank und die Software finden Sie im Installationshandbuch von ePolicy Orchestrator.

Mindestanforderungen an die Hardware

Hardware-Anforderungen und Netzwerkanforderungen für den Windows-Client für Workstations oder Server:

- Prozessor: Intel oder AMD x86 und x64.
- Freier Speicherplatz (Client): 15 MB, während der Installation jedoch 100 MB.
- Arbeitsspeicher: 256 MB RAM.
- Netzwerkumgebung: Microsoft- oder Novell NetWare-Netzwerke. Für NetWare-Netzwerke ist TCP/IP (Transmission Control Protocol/Internet Protocol) erforderlich.
- NIC: Netzwerkkarte; 10 Mb/s oder leistungsfähiger.

Unterstützte Betriebssysteme

Windows XP SP2, SP3 (nur 32-Bit-Version)

- Professional Edition

Windows Vista, Vista SP1 (32- und 64-Bit-Version)

- Business Edition
- Enterprise Edition
- Ultimate Edition

Windows 7 (32- und 64-Bit-Version)

- Professional Edition
- Enterprise Edition
- Ultimate Edition

Windows Server 2003 SP2, 2003 R2, 2003 R2 SP2 (32- und 64-Bit-Version)

- Alle Editionen

Windows Server 2008, 2008 SP1, 2008 SP2, 2008 R2 (32- und 64-Bit-Version)

- Alle Editionen

Unterstützte VPN-Clients (Virtual Private Network, virtuelles privates Netzwerk)

- AT&T Global Network Services-Client 7.6, 8.1
- CheckPoint VPN-Client R60, R71
- Cisco IPSec VPN-Client Version 5.0
- Cisco SSL VPN-Client 2.4
- Citrix SSL 4.5.6
- F5 Firepass 1200 6.1 (6031.2009.1010.312)
- iPass 3.5
- Juniper Netscreen VPN-Client 10.7
- Juniper Network Connect SSL VPN v6.4
- Microsoft Forefront UAG 2010
- Microsoft VPN
- NCP Secure Entry Client für Win32/64
- NetMotion Mobility XE 7.2
- Nortel Contivity VPN-Client 10.x
- SafeNet HARemote v2.0 VPN-Clients
- SonicWALL Global VPN-Client 4.0
- WatchGuard VPN

Unterstützte Virtualisierungsplattform

- VMware ESX 3.5, 4.0
- VMware Vsphere 4.0
- VMware View 4 3.1, 4.0
- VMware Thin App 4.0, 4.5
- VMware ACE 2.5 2.6
- VMware Workstation 6.5, 7.0
- VMware Player 2.5, 3.0
- VMware Server 1.0, 2.0
- Citrix Xen Server 5.0, 5.5
- Citrix Xen Desktop 3.0, 4.0
- Citrix Xen App 5.0, 6.0
- Microsoft Hyper-V Server 2008, 2008 R2

- Microsoft Windows Server 2008 Hyper-V 2008, 2008 R2
- Microsoft VDI (Bundle)
  - MED-V 1.0, 1.0 SP1
  - App-V 4.5, 4.6
  - SCVMM 2008, 2008 R2
  - SCCM 2007 SP2, 2007 R2
  - SCOM 2007, 2007 R2
- Microsoft App-V 4.5, 4.6
- XP Mode Windows 7 (32- und 64-Bit-Version)

Unterstützte Datenbanken

- MS SQL 2000
- MS SQL 2005
- MS SQL 2008, 2008 R2

Remote-Installation des Windows-Clients

Wenn Sie den Client über den ePO-Server ausbringen möchten, fügen Sie dem ePolicy Orchestrator-Master-Repository das zugehörige Ausbringungspaket hinzu und bringen es dann auf den Client-Computern aus. Ausführlichere Informationen finden Sie im *ePolicy Orchestrator-Produkthandbuch*.

Task

1. Wählen Sie die Optionsfolge **Software | Master-Repository**, und klicken Sie dann auf **Paket einchecken** (ePolicy Orchestrator 4.0), bzw. wählen Sie die Optionsfolge **Aktionen | Paket einchecken** (ePolicy Orchestrator 4.5 oder höher).
2. Wählen Sie **Produkt oder Aktualisierung (.ZIP)** aus, und klicken Sie dann auf **Durchsuchen**.
3. Machen Sie die .zip-Datei des Host IPS-Client-Pakets ausfindig, und klicken Sie dann auf **Öffnen**.
4. Klicken Sie auf **Weiter** und dann auf **Speichern**.
5. Wählen Sie die Optionsfolge **Systeme | Systemstruktur**, und wählen Sie dann die Systemgruppe aus, in der die Client-Komponente installiert werden soll.
6. Wechseln Sie zu **Client-Tasks**, und klicken Sie dann auf **Neuer Task** (ePolicy Orchestrator 4.0), bzw. wählen Sie die Optionsfolge **Aktionen | Neuer Task** (ePolicy Orchestrator 4.5 oder höher).
7. Vergeben Sie im Assistenten des Generators für Client-Tasks einen Namen für den Task, wählen Sie in der Task-Liste den Eintrag **Produktausbringung** aus, und klicken Sie dann auf **Weiter**.
8. Wählen Sie die Client-Plattform, dann **Host Intrusion Prevention 8.0** als das zu installierende Produkt, und klicken Sie auf **Weiter**.
9. Planen Sie die Ausführung des Tasks, klicken Sie auf **Weiter** und dann auf **Speichern**. Sollten Sie den Task zur sofortigen Ausführung vorgesehen haben, führen Sie die Agentenreaktivierung durch.

Lokale Installation des Windows-Clients

Sie können die Client-Software auch lokal, also ohne ePolicy Orchestrator zu verwenden, auf einer Windows-Workstation, einem Windows-Notebook oder einem Windows-Server installieren. Sie können dies manuell ausführen oder eine Drittanbieter-Software für die Verteilung auf eine Sammlung von Systemen verwenden.

Vorbereitung

Ist eine Vorgängerversion des Clients vorhanden, deaktivieren Sie unbedingt den IPS-Schutz, bevor Sie einen Installationsversuch unternehmen.

Task

1. Kopieren Sie die Client-Installationspaketdatei auf den Client-Computer.
2. Führen Sie das Installationsprogramm (McAfeeHip_ClientSetup.exe) im Paket aus.
3. Befolgen Sie die auf dem Bildschirm angezeigten Anweisungen, um die Installation fertigzustellen.

Anwenden von Richtlinien und IPS-Inhaltsaktualisierungen

Nach der Installation des Clients sollten Sie prüfen, ob Systeminformationen und Host Intrusion Prevention 8.0-Eigenschaften der ePO-Konsole (ePolicy Orchestrator) gemeldet werden. Einzelheiten finden Sie im *Produkthandbuch von ePolicy Orchestrator*.

Sie können jetzt IPS-Richtlinien für den Windows-Client überwachen und ausbringen. Einzelheiten finden Sie im *Host Intrusion Prevention 8.0-Produkthandbuch*.

Um sicherzustellen, dass der Client über die aktuellsten Inhalte verfügt, laden Sie das neueste Host Intrusion Prevention-Inhaltsaktualisierungspaket herunter und checken es zur Ausbringung in das ePO-Repository ein. Der Client kann Inhaltsaktualisierungen nur über den McAfee Agent-Befehl "Jetzt aktualisieren" abrufen, vorausgesetzt, der Host Intrusion Prevention-Administrator hat den Aktualisierungsprozess entsprechend konfiguriert. Einzelheiten zu diesen Vorgängen finden Sie im Abschnitt *Aktualisierungen zum Host IPS-Schutz* im *McAfee Host Intrusion Prevention-Produkthandbuch*.

Befolgen Sie die im *ePolicy Orchestrator-Produkthandbuch* aufgeführten Vorgehensweisen bei der Ausbringung von Produkt-Patches und Produktaktualisierungen über die ePO-Konsole.

Achten Sie beim Installieren von Produkt-Patches/Produktaktualisierungen stets darauf, dass der IPS-Schutz nicht aktiviert ist, und befolgen Sie die in diesem Kapitel erläuterten Schritte zur Produktinstallation.

McAfee stellt ein Dienstprogramm (client_control.exe) zur Automatisierung von Aktualisierungen und anderen Wartungs-Tasks bereit, für den Fall, dass Host Intrusion Prevention mithilfe von Drittanbieter-Software auf Client-Computern installiert wird. Dieses im Client-Paket erhältliche Befehlzeilendienstprogramm lässt sich in Installations- und Wartungsskripte einbinden, um den IPS-Schutz vorübergehend zu deaktivieren und Protokollierungsfunktionen zu aktivieren. Weitere Hinweise zur Nutzung, einschließlich verwendeter Parameter und Sicherheitsinformationen, finden Sie in *Anhang B – Dienstprogramm "Clientcontrol.exe"* des *McAfee Host Intrusion Prevention-Produkthandbuchs*.

Entfernen des Windows-Clients

Der Host Intrusion Prevention-Client kann per Remote-Vorgang entfernt werden. Führen Sie hierzu über den ePolicy Orchestrator-Server oder direkt auf dem Client-Computer einen Ausbringungs-Task aus.

Über den ePO-Server

- Führen Sie einen Ausbringungs-Task für den Client aus, und wählen Sie als Aktion für Host Intrusion Prevention die Option **Entfernen** aus.

Direkt auf dem Client-Computer

Ist der Zugriff auf die Client-Konsole über das Symbol in der Taskleiste nicht möglich, ändern Sie dies entsprechend, um das Entfernen des Clients zu ermöglichen.

Task

1. Wählen Sie über den ePO-Server das System aus, von dem Sie die Software entfernen möchten.
2. Erzwingen Sie die Richtlinienoption **Produkt in der Liste "Software" anzeigen** der Host Intrusion Prevention-Benutzeroberfläche.
3. Legen Sie für den Ausbringungs-Task für Host Intrusion Prevention den Wert **Ignorieren** fest.
4. Entsperren Sie auf dem Client-Computer die Client-Schnittstelle mit dem entsprechenden Kennwort.
5. Heben Sie die Auswahl von **Host-IPS aktivieren** auf.
6. Verwenden Sie die Option **Software** in der Systemsteuerung, um Host Intrusion Prevention zu entfernen.
7. Starten Sie den Computer neu.

Fehlerbehebung bei Windows-Installationsproblemen

Wenn während der Installation oder Deinstallation des Clients ein Problem aufgetreten ist, gilt es mehrere Punkte zu prüfen. So können Sie beispielsweise sicherstellen, dass alle erforderlichen Dateien im richtigen Verzeichnis installiert wurden und dass der Client ausgeführt wird. Zudem können Sie die Prozessprotokolle zurate ziehen.

Überprüfen der Windows-Installationsdateien

Vergewissern Sie sich nach der Installation, dass Ordner und Dateien auf dem Client installiert wurden. Der Ordner C:\Programme\McAfee\Host Intrusion Prevention sollte installiert worden sein und folgende grundlegenden Dateien und Ordner enthalten:

Dateiname	Beschreibung
FireSvc.exe, VSCore/Release/mfefire.exe, VSCore/Release/mfrvtp.exe	Host Intrusion Prevention-Dienste
McAfeeFire.exe	Client-Konsole

Der Installationsverlauf wird in die Datei C:\Windows\Temp\McAfeeLogs\McAfeeHip8_Install_<version>.log geschrieben. Mit folgendem Eintrag in der Datei wird die vorschriftsmäßige Installation des Clients sichergestellt: *Product: McAfee Host Intrusion Prevention -- Installation operation completed successfully* (Produkt: McAfee Host Intrusion Prevention – Installation erfolgreich abgeschlossen).

Protokolldateien sind unter Vista und Windows 7 im Verzeichnis C:\Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\McAfee\Host Intrusion Prevention\ bzw. C:\ProgramData\McAfee\Host Intrusion Prevention zu finden.

Überprüfen, ob der Windows-Client ausgeführt wird

Auch wenn der Client ordnungsgemäß installiert ist, können während des Betriebs Probleme auftreten. Wenn der Client beispielsweise nicht in der ePO-Konsole angezeigt wird, überprüfen Sie, ob er ausgeführt wird: Öffnen Sie eine Eingabeaufforderung, geben Sie tasklist \svc ein, und stellen Sie sicher, dass die folgenden Dienste ausgeführt werden:

- FireSvc.exe
- mfefire.exe
- mfevtp.exe

Ist dies nicht der Fall, gehen Sie wie folgt vor:

1. Führen Sie die unter **C:\Programme\McAfee\Host Intrusion Prevention** zu findende Datei McAfeeFire.exe aus, um die Client-Konsole aufzurufen.
2. Entsperren Sie die Konsole: Wählen Sie die Optionsfolge **Task | Sperrung der Benutzeroberfläche aufheben**, und geben Sie "abcde12345" als standardmäßiges Kennwort ein.
3. Legen Sie die Debugging-Einstellungen fest: Wählen Sie die Optionsfolge **Hilfe | Fehlerbehebung**, und aktivieren Sie die vollständige Debug-Protokollierung für Firewall und IPS.
4. Vergewissern Sie sich, dass sowohl das Eindringungsschutzsystem auf Host-Ebene als auch die Funktion für Netzwerk-IPS deaktiviert sind.
5. Öffnen Sie eine Eingabeaufforderung, und führen Sie net start enterceptagent aus, um den Client-Dienst aufzurufen.

Wird der Dienst nach wie vor nicht aufgerufen, sehen Sie in der Datei FireSvc.log nach, ob es Fehler- oder Warnmeldungen gibt, die möglicherweise Aufschluss darüber geben, warum dies der Fall ist.

Überprüfen, dass Ereignisse hinsichtlich des Eindringungsschutzsystems auf Host-Ebene vorschriftsmäßig ausgelöst werden

Nachdem Sie sich vergewissert haben, dass der Client ordnungsgemäß installiert wurde und ausgeführt wird, müssen Sie prüfen, ob der IPS-Schutz erwartungsgemäß funktioniert. Stellen Sie zunächst sicher, dass das Eindringungsschutzsystem auf Host-Ebene aktiviert ist (in der Client-Konsole). Erstellen Sie dann ein neues Textdokument im Client-Installationsverzeichnis: C:\Programme\McAfee\Host Intrusion Prevention. Diese Aktion sollte unterbunden werden, und es sollte eine Fehlermeldung ausgegeben werden, die besagt, dass Sie zum Speichern an diesem Speicherort nicht berechtigt sind. Ziehen Sie die Datei HipShield.log zurate, und durchsuchen Sie sie von unten nach oben nach einem Verstoß. Vergewissern Sie sich, dass folgende Signatur ausgelöst wurde: 1001 Windows Agent Shielding -- File Modification (1001 Windows Agent-Abschirmung – Dateimodifizierung).

Anhalten des Windows-Clients

Im Rahmen der Fehlerbehebung müssen Sie einen derzeit ausgeführten Client möglicherweise anhalten und neu starten.

Task

1. Deaktivieren Sie den IPS-Schutz, wenn er aktiviert ist. Verwenden Sie eine der folgenden Vorgehensweisen:
   - Legen Sie in der ePO-Konsole für **IPS-Optionen** den Wert **Aus** fest, und wenden Sie dann die Richtlinie auf den Client an.
   - Rufen Sie die Client-Konsole auf, und deaktivieren Sie auf der Registerkarte für die IPS-Richtlinie die Option **Host-IPS aktivieren**.

   HINWEIS: Die Deaktivierung des Firewall-Schutzes ist zum Anhalten des Clients nicht erforderlich.
2. Öffnen Sie eine Eingabeaufforderung, und führen Sie folgenden Befehl aus: net stop enterceptagent.

Neustarten des Windows-Clients

Im Rahmen der Fehlerbehebung müssen Sie einen zuvor angehaltenen Client möglicherweise neu starten.

Task

1. Öffnen Sie eine Eingabeaufforderung, und führen Sie folgenden Befehl aus: net start enterceptagent.
2. Wenn Sie den IPS-Schutz deaktiviert haben, aktivieren Sie ihn mithilfe einer der folgenden Methoden erneut:
   - Legen Sie in der ePO-Konsole für **IPS-Optionen** den Wert **Ein** fest, und wenden Sie dann die Richtlinie auf den Client an.
   - Rufen Sie die Client-Konsole auf, und aktivieren Sie auf der Registerkarte für die IPS-Richtlinie die Option **Host-IPS aktivieren**.

Installieren des Solaris-Clients

In diesem Abschnitt finden Sie Informationen zu den Anforderungen und Eigenschaften sowie zur Installation des McAfee Host Intrusion Prevention 8.0-Solaris-Clients, der potentiell schädliche Versuche, die Dateien und Anwendungen auf einem Solaris-Server zu manipulieren, erkennt und unterbindet. Der Client schützt das Betriebssystem des Servers sowie Apache- und Sun-Web-Server, wobei verstärkt auf das Verhindern von Buffer Overflow-Angriffen geachtet wird.

Inhalt

- Details zum Solaris-Client
- Anwenden von Richtlinien und IPS-Inhaltsaktualisierungen
- Entfernen des Solaris-Clients
- Fehlerbehebung bei Solaris-Installationsproblemen
- Anhalten des Solaris-Clients
- Neustarten des Solaris-Clients

Details zum Solaris-Client

Der Host Intrusion Prevention 8.0-Client für Solaris kann mit ePolicy Orchestrator 4.0 und höher, McAfee Agent 4.0 und der Host Intrusion Prevention 8.0-Verwaltungskomponente verwendet werden. Detaillierte Informationen zur Installation und Verwendung von ePolicy Orchestrator finden Sie im Installationshandbuch von ePolicy Orchestrator.

Mindestanforderungen an die Hardware

- SPARC sun4u/sun4v (32- und 64-Bit-Plattform)
- 256 MB RAM
- 10 MB freier Speicherplatz auf der Festplatte

Unterstützte Betriebssysteme

- SPARC Solaris 9, sun4u (32-Bit oder 64-Bit-Kernel)
- SPARC Solaris 10, sun4u, sun4v (64-Bit-Kernel)

Unterstützte Web-Server

- Apache-Web-Server ab Version 1.3.6
- Apache-Web-Server ab Version 2.0.42
- Apache-Web-Server ab Version 2.2.3
- Sun Java Web Server 6.1

- Sun Java Web Server 7.0

Richtlinienerzwingung

Für den Solaris-Client stehen nicht alle Host Intrusion Prevention 8.0-Richtlinien zur Verfügung. Host Intrusion Prevention schützt also den Host-Server vor schädlichen Angriffen, bietet jedoch keinen Firewall-Schutz. Die gültigen Richtlinien sind hier aufgelistet.

Richtlinie	Verfügbare Optionen
HIP 8.0 ALLGEMEIN:	
Client-UI	Nur **Administrator** bzw. **Zeitbasiertes Kennwort**, zur Nutzung des Tools zur Fehlerbehebung**.**
Vertrauenswürdige Netzwerke	Keine
Vertrauenswürdige Anwendungen	Alle außer **Für Firewall als vertrauenswürdig markieren**.
HIP 8.0 IPS:	
IPS-Optionen	• **Host-IPS aktivieren** • **Adaptiven Modus aktivieren** • **Bestehende Client-Regeln beibehalten**
IPS-Schutz	Alle
IPS-Regeln	• **Ausnahmeregeln** • **Signaturen** (nur standardmäßige und benutzerdefinierte HIPS-Regeln) HINWEIS: NIPS-Signaturen und **Anwendungsschutzregeln** sind nicht verfügbar.
IPS-Ereignisse	Alle
IPS-Client-Regeln	Alle
HIP 8.0 FIREWALL:	
Firewall-Optionen	Keine
Firewall-Regeln	Keine
Firewall-DNS-Blockierung	Keine

HINWEIS: Der Client unterstützt sowohl globale als auch lokale Zonen. Die Installation erfolgt ausschließlich in der globalen Zone.

Solaris-Zonenunterstützung

Der Client unterstützt sowohl den Schutz globaler als auch lokaler Zonen, wird jedoch stets in der globalen Zone installiert. Zur Beschränkung des Schutzes auf bestimmte Zonen werden die Signaturen der IPS-Regelrichtlinien bearbeitet. Hierbei wird ein Zonenabschnitt hinzugefügt und der Name der Zone als Wert aufgenommen.

Wenn Sie beispielsweise über eine Zone namens "app_zone" verfügen, deren Stammverzeichnis (Root) "/zones/app" lautet, gilt die Signaturregel nur für die Datei in der Zone "app_zone", nicht in der globalen Zone. Beachten Sie, dass in dieser Version der Web-Server-Schutz nicht auf eine bestimmte Zone beschränkt werden kann. Der Code für diese Regel würde wie folgt lauten:

Rule {

...

file { Include "/tmp/test.log" }

zone { Include "app_zone" }

... }

Weitere Informationen zur Bearbeitung von Signaturen finden Sie im Produkthandbuch bzw. in der Hilfe in *Anhang A – Schreiben von benutzerdefinierten Signaturen*.

Remote-Installation des Solaris-Clients

Wenn Sie den Client über den ePO-Server ausbringen möchten, fügen Sie dem ePolicy Orchestrator-Master-Repository das zugehörige Ausbringungspaket hinzu und bringen es dann auf den Client-Computern aus. Ausführlichere Informationen finden Sie im *ePolicy Orchestrator-Produkthandbuch*.

Task

1. Wählen Sie die Optionsfolge **Software | Master-Repository**, und klicken Sie dann auf **Paket einchecken** (ePolicy Orchestrator 4.0), bzw. wählen Sie die Optionsfolge **Aktionen | Paket einchecken** (ePolicy Orchestrator 4.5 oder höher).
2. Wählen Sie **Produkt oder Aktualisierung (.ZIP)** aus, und klicken Sie dann auf **Durchsuchen**.
3. Machen Sie die .zip-Datei des Host IPS-Client-Pakets ausfindig, und klicken Sie dann auf **Öffnen**.
4. Klicken Sie auf **Weiter** und dann auf **Speichern**.
5. Wählen Sie die Optionsfolge **Systeme | Systemstruktur**, und wählen Sie dann die Systemgruppe aus, in der die Client-Komponente installiert werden soll.
6. Wechseln Sie zu **Client-Tasks**, und klicken Sie dann auf **Neuer Task** (ePolicy Orchestrator 4.0), bzw. wählen Sie die Optionsfolge **Aktionen | Neuer Task** (ePolicy Orchestrator 4.5 und höher).
7. Vergeben Sie im Assistenten des Generators für Client-Tasks einen Namen für den Task, wählen Sie in der Task-Liste den Eintrag **Produktausbringung** aus, und klicken Sie dann auf **Weiter**.
8. Wählen Sie die Client-Plattform, dann **Host Intrusion Prevention 8.0** als das zu installierende Produkt, und klicken Sie auf **Weiter**.
9. Planen Sie die Ausführung des Tasks, klicken Sie auf **Weiter** und dann auf **Speichern**. Sollten Sie den Task zur sofortigen Ausführung vorgesehen haben, führen Sie die Agentenreaktivierung durch.

Lokale Installation des Solaris-Clients

Sie können die Client-Software auch lokal, also ohne ePolicy Orchestrator zu verwenden, auf einem Solaris-Server installieren. Kopieren Sie hierzu die Client-Installationsdatei auf den Client-Computer, und führen Sie den entsprechenden Befehl aus. Ist eine Vorgängerversion des Clients vorhanden, deaktivieren Sie unbedingt den IPS-Schutz, bevor Sie einen Installationsversuch unternehmen.

HINWEIS: Der Client kann nur in der globalen Zone installiert werden, unterstützt jedoch lokale Zonen.

Task

1. Laden Sie die Dateien **MFEhip.pkg** und **install_hip_solaris** aus dem Client-Installationspaket herunter.
2. Melden Sie sich als Root-Benutzer an, und führen Sie folgenden Befehl aus: ./install_hip_solaris MFEhip.pkg

Anwenden von Richtlinien und IPS-Inhaltsaktualisierungen

Nach der Installation des Clients sollten Sie prüfen, ob Systeminformationen und Host Intrusion Prevention 8.0-Eigenschaften dem ePO-Server (ePolicy Orchestrator) gemeldet werden. Einzelheiten finden Sie im *Produkthandbuch von ePolicy Orchestrator*.

Sie können jetzt IPS-Richtlinien für den Solaris-Client überwachen und ausbringen. Einzelheiten finden Sie im *McAfee Host Intrusion Prevention 8.0-Produkthandbuch*.

Um sicherzustellen, dass der Client über die aktuellsten Inhalte verfügt, laden Sie das neueste Host Intrusion Prevention-Inhaltsaktualisierungspaket herunter und checken es zur Ausbringung in das ePO-Repository ein. Einzelheiten zu diesem Vorgang finden Sie im Abschnitt *Aktualisierungen zum Host IPS-Schutz* im *McAfee Host Intrusion Prevention-Produkthandbuch*.

Entfernen des Solaris-Clients

Der Host Intrusion Prevention-Client kann per Remote-Vorgang entfernt werden. Führen Sie hierzu über den ePolicy Orchestrator-Server oder direkt auf dem Client-Computer einen Ausbringungs-Task aus.

Über den ePO-Server

- Führen Sie einen Ausbringungs-Task für den Client aus, und wählen Sie als Aktion für Host Intrusion Prevention die Option **Entfernen** aus.

Direkt auf dem Client-Computer

Vor dem manuellen Entfernen vom Client-Computer müssen Sie zunächst die IPS-Richtlinien des Clients über den ePO-Server deaktivieren.

- Melden Sie sich als Root-Benutzer beim Client-Computer an, und führen Sie folgenden Befehl aus: /opt/McAfee/hip/install_hip_solaris -uninstall

Fehlerbehebung bei Solaris-Installationsproblemen

Wenn während der Installation oder Deinstallation des Clients ein Problem aufgetreten ist, gilt es mehrere Punkte zu prüfen. So können Sie beispielsweise sicherstellen, dass alle erforderlichen Dateien im richtigen Verzeichnis installiert wurden und dass der Client ausgeführt wird. Zudem können Sie die Prozessprotokolle zurate ziehen.

Überprüfen der Solaris-Installationsdateien

Nach der Installation sollten Sie überprüfen, ob alle Dateien im richtigen Verzeichnis auf dem Client installiert wurden. Das Verzeichnis opt/McAfee/hip sollte folgende grundlegenden Dateien und Verzeichnisse enthalten:

Datei-/Verzeichnisname	Beschreibung
HipClient; HipClient-bin	Solaris-Client
HipClientPolicy.xml	Richtlinienregeln
hipts; hipts-bin	Fehlerbehebungs-Tool
*.so	Gemeinsame Objektmodule von Host Intrusion Prevention und ePO
Protokollverzeichnis	Enthält folgende Protokolldateien: HIPShield.log und HIPClient.log

Der Installationsverlauf wird in die Datei /opt/McAfee/etc/hip-install.log geschrieben. Lesen Sie in dieser Datei nach, wenn Sie Fragen zur Installation oder Entfernung des Host Intrusion Prevention-Clients haben.

Überprüfen, ob der Solaris-Client ausgeführt wird

Auch wenn der Client ordnungsgemäß installiert ist, können während des Betriebs Probleme auftreten. Wenn der Client beispielsweise nicht in der ePO-Konsole angezeigt wird, überprüfen Sie mithilfe eines der folgenden Befehle, ob er ausgeführt wird:

- /etc/rc2.d/S99hip status
- ps –ef | grep hip

Anhalten des Solaris-Clients

Im Rahmen der Fehlerbehebung müssen Sie einen derzeit ausgeführten Client möglicherweise anhalten und neu starten.

Task

1. Deaktivieren Sie den IPS-Schutz. Verwenden Sie eine der folgenden Vorgehensweisen:
   - Legen Sie in der ePO-Konsole für **IPS-Optionen** den Wert **Aus** fest, und wenden Sie dann die Richtlinie auf den Client an.
   - Melden Sie sich als Root-Benutzer an, und führen Sie folgenden Befehl aus: hipts engines MISC:off
2. Führen Sie folgenden Befehl aus: /etc/rc2.d/S99hip stop

Neustarten des Solaris-Clients

Im Rahmen der Fehlerbehebung müssen Sie einen derzeit ausgeführten Client möglicherweise anhalten und neu starten.

Task

1. Führen Sie folgenden Befehl aus: /etc/rc2.d/S99hip restart

2 Aktivieren Sie den IPS-Schutz. Gehen Sie gemäß einer der nachfolgenden Methoden vor, je nachdem, mit welcher Sie den Client angehalten haben:

- Legen Sie in der ePO-Konsole für **IPS-Optionen** den Wert **Ein** fest, und wenden Sie dann die Richtlinie auf den Client an.
- Melden Sie sich als Root-Benutzer an, und führen Sie folgenden Befehl aus: hipts engines MISC:on

Installieren des Linux-Clients

In diesem Abschnitt finden Sie Informationen zu den Anforderungen und Eigenschaften sowie zur Installation des McAfee Host Intrusion Prevention 8.0-Linux-Clients, der potentiell schädliche Versuche, die Dateien und Anwendungen auf einem Linux-Server zu manipulieren, erkennt und unterbindet.

Inhalt

- Details zum Linux-Client
- Anwenden von Richtlinien und IPS-Inhaltsaktualisierungen
- Entfernen des Linux-Clients
- Fehlerbehebung bei Linux-Installationsproblemen
- Anhalten des Linux-Clients
- Neustarten des Linux-Clients

Details zum Linux-Client

Der Host Intrusion Prevention 8.0-Client für Linux kann mit ePolicy Orchestrator 4.0 und höher, McAfee Agent 4.0 und der Host Intrusion Prevention 8.0-Verwaltungskomponente verwendet werden. Detaillierte Informationen zur Installation und Verwendung von ePolicy Orchestrator finden Sie im Installationshandbuch von ePolicy Orchestrator.

Mindestanforderungen an die Hardware

- Intel oder AMD x86 und x64
- 512 MB RAM
- 20 MB freier Speicherplatz auf der Festplatte

Unterstützte Betriebssysteme

- Red Hat Linux Enterprise 4, 32-Bit-Version
  - 2.6.9-5.EL
  - 2.6.9-5.Elhugemem
  - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 4, 64-Bit-Version
  - 2.6.9-5.EL
  - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 5, 32-Bit-Version
  - 2.6.18-8.el5

  - 2.6.18-8.el5PAE
- Red Hat Linux Enterprise 5, 64-Bit-Version
  - 2.6.18-8.el5
- SUSE Linux Enterprise 10, 32-Bit-Version
  - 2.6.16.21-0.8-bigsmp
  - 2.6.16.21-0.8-default
  - 2.6.16.21-0.8-smp
- SUSE Linux Enterprise 10, 64-Bit-Version
  - 2.6.16.21-0.8-default
  - 2.6.16.21-0.8-smp
- SUSE Linux Enterprise 11, 32-Bit-Version
  - 2.6.27.19-5-default
  - 2.6.27.19-5-pae
- SUSE Linux Enterprise 11, 64-Bit-Version
  - 2.6.27.19-5-default

Unterstützte Web-Server

- Apache-Web-Server ab Version 1.3.6
- Apache-Web-Server ab Version 2.0.42
- Apache-Web-Server ab Version 2.2.3

Dateisystemschutz und HTTP-Schutz

Der Linux-Client schützt Betriebssystemdateien und -prozesse. Er bietet keinen Netzwerkschutz, keinen Buffer Overflow-Schutz und keine Überwachung des HTTP-Verkehrs.

Richtlinienerzwingung mit dem Linux-Client

Für den Linux-Client stehen nicht alle Host Intrusion Prevention 8.0-Richtlinien zur Verfügung. Host Intrusion Prevention schützt also den Host-Server vor schädlichen Angriffen, bietet jedoch keinen Firewall-Schutz. Die gültigen Richtlinien sind hier aufgelistet.

Richtlinie	**Verfügbare Optionen**
HIP 8.0 ALLGEMEIN:	
Client-UI	Nur **Administrator** bzw. **Zeitbasiertes Kennwort**, zur Nutzung des Tools zur Fehlerbehebung**.**
Vertrauenswürdige Netzwerke	Keine
Vertrauenswürdige Anwendungen	Alle außer **Für Firewall als vertrauenswürdig markieren**.
HIP 8.0 IPS:	
IPS-Optionen	• **HIPS aktivieren** • **Adaptiven Modus aktivieren** • **Bestehende Client-Regeln beibehalten**
IPS-Schutz	Alle

Richtlinie	Verfügbare Optionen
IPS-Regeln	• **Ausnahmeregeln** • **Signaturen** (nur standardmäßige und benutzerdefinierte HIPS-Regeln) HINWEIS: NIPS-Signaturen und **Anwendungsschutzregeln** sind nicht verfügbar.
IPS-Ereignisse	Alle
IPS-Client-Regeln	Alle
HIP 8.0 FIREWALL:	
Firewall-Optionen	Keine
Firewall-Regeln	Keine
Firewall-DNS-Blockierung	Keine

Remote-Installation des Linux-Clients

Wenn Sie den Client über den ePO-Server ausbringen möchten, fügen Sie dem ePolicy Orchestrator-Master-Repository das zugehörige Ausbringungspaket hinzu und bringen es dann auf den Client-Computern aus. Ausführlichere Informationen finden Sie im *ePolicy Orchestrator-Produkthandbuch*.

Task

1. Wählen Sie die Optionsfolge **Software | Master-Repository**, und klicken Sie dann auf **Paket einchecken** (ePolicy Orchestrator 4.0), bzw. wählen Sie die Optionsfolge **Aktionen | Paket einchecken** (ePolicy Orchestrator 4.5 oder höher).
2. Wählen Sie **Produkt oder Aktualisierung (.ZIP)** aus, und klicken Sie dann auf **Durchsuchen**.
3. Machen Sie die .zip-Datei des Host IPS-Client-Pakets ausfindig, und klicken Sie dann auf **Öffnen**.
4. Klicken Sie auf **Weiter** und dann auf **Speichern**.
5. Wählen Sie die Optionsfolge **Systeme | Systemstruktur**, und wählen Sie dann die Systemgruppe aus, in der die Client-Komponente installiert werden soll.
6. Wechseln Sie zu **Client-Tasks**, und klicken Sie dann auf **Neuer Task** (ePolicy Orchestrator 4.0), bzw. wählen Sie die Optionsfolge **Aktionen | Neuer Task** (ePolicy Orchestrator 4.5 und höher).
7. Vergeben Sie im Assistenten des Generators für Client-Tasks einen Namen für den Task, wählen Sie in der Task-Liste den Eintrag **Produktausbringung** aus, und klicken Sie dann auf **Weiter**.
8. Wählen Sie die Client-Plattform, dann **Host Intrusion Prevention 8.0.0** als das zu installierende Produkt, und klicken Sie auf **Weiter**.

9 Planen Sie die Ausführung des Tasks, klicken Sie auf **Weiter** und dann auf **Speichern**. Sollten Sie den Task zur sofortigen Ausführung vorgesehen haben, führen Sie die Agentenreaktivierung durch.

HINWEIS: Wenn Sie den Client von Version 7.1.0 aktualisieren möchten, müssen Sie das Linux-System neu starten.

Lokale Installation des Linux-Clients

Sie können die Client-Software auch direkt, also ohne ePolicy Orchestrator zu verwenden, auf einem Solaris-Server installieren. Kopieren Sie hierzu die Client-Installationsdatei auf den Client-Computer, und führen Sie den entsprechenden Befehl aus. Ist eine Vorgängerversion des Clients vorhanden, deaktivieren Sie unbedingt den IPS-Schutz, bevor Sie einen Installationsversuch unternehmen.

Task

1 Kopieren Sie die entsprechende .rpm-Datei aus dem Client-Installationspaket auf das Linux-System:

- Red Hat Linux Enterprise 4, 32-Bit-Version
  1. MFEhiplsm-kernel-8.0.0.-<build-nummer>.RH4.i386.rpm
  2. MFEhiplsm-8.0.0.-<build-nummer>.RH4.i386.rpm
- Red Hat Linux Enterprise 4, 64-Bit-Version
  1. MFEhiplsm-kernel-8.0.0.-<build-nummer>.RH4.x86_64.rpm
  2. MFEhiplsm-apache-8.0.0.-<build-nummer>.RH4.x86_64.rpm
  3. MFEhiplsm-8.0.0.-<build-nummer>.RH4.i386.rpm
- Red Hat Linux Enterprise 5, 32-Bit-Version
  1. MFEhiplsm-kernel-8.0.0.-<build-nummer>.RH5.i386.rpm
  2. MFEhiplsm-8.0.0.-<build-nummer>.RH5.i386.rpm
- Red Hat Linux Enterprise 5, 64-Bit-Version
  1. MFEhiplsm-kernel-8.0.0.-<build-nummer>.RH5.x86_64.rpm
  2. MFEhiplsm-apache-8.0.0.-<build-nummer>.RH5.x86_64.rpm
  3. MFEhiplsm-8.0.0.-<build-nummer>.RH5.i386.rpm
- SUSE Linux Enterprise 10, 32-Bit-Version
  1. MFEhiplsm-kernel-8.0.0.-<build-nummer>.SUSE10.i386.rpm
  2. MFEhiplsm-8.0.0.-<build-nummer>.SUSE10.i386.rpm
- SUSE Linux Enterprise 10, 64-Bit-Version
  1. MFEhiplsm-kernel-8.0.0.-<build-nummer>.SUSE10.x86_64.rpm
  2. MFEhiplsm-apache-8.0.0.-<build-nummer>.SUSE10.x86_64.rpm
  3. MFEhiplsm-8.0.0.-<build-nummer>.SUSE10.i386.rpm
- SUSE Linux Enterprise 11, 32-Bit-Version
  1. MFEhiplsm-kernel-8.0.0.-<build-nummer>.SUSE11.i386.rpm
  2. MFEhiplsm-8.0.0.-<build-nummer>.SUSE11.i386.rpm

- SUSE Linux Enterprise 11, 64-Bit-Version
  1. MFEhiplsm-kernel-8.0.0.-<build-nummer>.SUSE11.x86_64.rpm
  2. MFEhiplsm-apache-8.0.0.-<build-nummer>.SUSE11.x86_64.rpm
  3. MFEhiplsm-8.0.0.-<build-nummer>.SUSE11.i386.rpm

2. Führen Sie folgenden Befehl aus: rpm -i <name der rpm-datei>, und zwar für jede RPM-Datei, in der angegebenen Reihenfolge.

   HINWEIS: Wenn Sie den Client von Version 7.1.0 aktualisieren möchten, müssen Sie das Linux-System neu starten.

Anwenden von Richtlinien und IPS-Inhaltsaktualisierungen

Nach der Installation des Clients sollten Sie prüfen, ob Systeminformationen und Host Intrusion Prevention 8.0-Eigenschaften dem ePO-Server (ePolicy Orchestrator) gemeldet werden. Einzelheiten finden Sie im *Produkthandbuch von ePolicy Orchestrator*.

Sie können jetzt IPS-Richtlinien für den Linux-Client überwachen und ausbringen. Einzelheiten finden Sie im *Host Intrusion Prevention 8.0-Produkthandbuch*.

Um sicherzustellen, dass der Client über die aktuellsten Inhalte verfügt, laden Sie das neueste Host Intrusion Prevention-Inhaltsaktualisierungspaket herunter und checken es zur Ausbringung in das ePO-Repository ein. Einzelheiten zu diesen Vorgängen finden Sie im *Produkthandbuch von ePolicy Orchestrator*.

Um sicherzustellen, dass der Client über die neuesten IPS-Inhalte verfügt, laden Sie das neueste Host Intrusion Prevention-Inhaltsaktualisierungspaket herunter und checken es zur Ausbringung in das ePO-Repository ein. Einzelheiten zu diesen Vorgängen finden Sie im Abschnitt *Aktualisierungen zum Host IPS-Schutz* im *McAfee Host Intrusion Prevention-Produkthandbuch*.

Entfernen des Linux-Clients

Der Host Intrusion Prevention-Client kann per Remote-Vorgang entfernt werden. Führen Sie hierzu über den ePolicy Orchestrator-Server oder direkt auf dem Client-Computer einen Ausbringungs-Task aus.

Über den ePO-Server

- Führen Sie einen Ausbringungs-Task für den Client aus, und wählen Sie als Aktion für Host Intrusion Prevention die Option **Entfernen** aus.

Direkt auf dem Client-Computer

Vor dem manuellen Entfernen vom Client-Computer müssen Sie zunächst die IPS-Richtlinien des Clients über den ePO-Server deaktivieren.

- Melden Sie sich als Root-Benutzer beim Client-Computer an, und führen Sie folgenden Befehl aus: rpm -e MFEhiplsm; MFEhiplsm-kernel; MFEhiplsm-apache

Fehlerbehebung bei Linux-Installationsproblemen

Wenn während der Installation oder Deinstallation des Clients ein Problem aufgetreten ist, gilt es mehrere Punkte zu prüfen. So können Sie beispielsweise sicherstellen, dass alle erforderlichen Dateien im richtigen Verzeichnis installiert wurden und dass der Client ausgeführt wird. Zudem können Sie die Prozessprotokolle zurate ziehen.

Überprüfen der Linux-Installationsdateien

Nach der Installation sollten Sie überprüfen, ob alle Dateien im richtigen Verzeichnis auf dem Client installiert wurden. Das Verzeichnis opt/McAfee/hip sollte folgende grundlegenden Dateien und Verzeichnisse enthalten:

Datei-/Verzeichnisname	Beschreibung
HipClient; HipClient-bin	Linux-Client
HipClientPolicy.xml	Richtlinienregeln
hipts; hipts-bin	Fehlerbehebungs-Tool
*.so	Gemeinsame Objektmodule von Host Intrusion Prevention und ePO
Protokollverzeichnis	Enthält folgende Protokolldateien: HIPShield.log und HIPClient.log

Der Installationsverlauf wird in die Datei /opt/McAfee/etc/hip-install.log geschrieben. Lesen Sie in dieser Datei nach, wenn Sie Fragen zur Installation oder Entfernung des Host Intrusion Prevention-Clients haben.

Überprüfen, ob der Linux-Client ausgeführt wird

Auch wenn der Client ordnungsgemäß installiert ist, können während des Betriebs Probleme auftreten. Wenn der Client beispielsweise nicht in der ePO-Konsole angezeigt wird, überprüfen Sie mit folgendem Befehl, ob er ausgeführt wird: ps –ef | grep hip

Anhalten des Linux-Clients

Im Rahmen der Fehlerbehebung müssen Sie einen derzeit ausgeführten Client möglicherweise anhalten und neu starten.

Task

1. Wenn Sie einen derzeit ausgeführten Client anhalten möchten, deaktivieren Sie zunächst den IPS-Schutz. Verwenden Sie eine der folgenden Vorgehensweisen:
   - Legen Sie in der ePO-Konsole für **IPS-Optionen** den Wert **Aus** fest, und wenden Sie dann die Richtlinie auf den Client an.
   - Melden Sie sich als Root-Benutzer an, und führen Sie folgenden Befehl aus: hipts engines MISC:off
2. Führen Sie folgenden Befehl aus: hipts agent off

Neustarten des Linux-Clients

Im Rahmen der Fehlerbehebung müssen Sie einen derzeit ausgeführten Client möglicherweise anhalten und neu starten.

Task

1. Um einen Client neu zu starten, führen Sie folgenden Befehl aus: hipts agent on
2. Aktivieren Sie den IPS-Schutz. Gehen Sie gemäß einer der nachfolgenden Methoden vor, je nachdem, mit welcher Sie den Client angehalten haben:
   - Legen Sie in der ePO-Konsole für **IPS-Optionen** den Wert **Ein** fest, und wenden Sie dann die Richtlinie auf den Client an.
   - Melden Sie sich als Root-Benutzer an, und führen Sie folgenden Befehl aus: hipts engines MISC:on